Description of document:	**The Achievements of the Signal Security Agency (SSA) in World War II, 1946 provided by The National Security Agency (NSA), 2010**
Requested date:	21-August-2010
Released date:	08-October-2010
Posted date:	25-October-2010
Source of document:	National Security Agency Declassification Services (DJ5) Suite 6884, Bldg. SAB2 9800 Savage Road Ft. George G. Meade, MD, 20755-6884

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 62647
8 October 2010

This is an initial response to your Freedom of Information Act (FOIA) request submitted via the Internet on 21 August 2010, which was received by this office on 23 August 2010, for "A document or documents that provide a general description of SIGNIN (a WWII era machine)." Your request has been assigned Case Number 62647. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you.

For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. You must pay for search time in excess of 2 hours and duplication in excess of 100 pages. At this stage of processing, the fees are minimal; therefore, we are not assessing any fees.

In our preliminary search, we located one document that is responsive to your request, "Achievements of the Signal Security Agency in World War II." The document was reviewed under the previous Executive Order (E.O. 12958, as amended) in January 2009. That document is enclosed and is being released to you just as it was released in FOIA Case 53751. If you would like to have the document re-reviewed under the new Executive Order, please so notify us.

We consider the enclosed document to be responsive to your request in that it does describe the machine, as you requested. It also includes a picture of the machine. If you are interested in four additional documents that we located in our preliminary search (within your two free hours of search), you will be responsible for all of the duplication. Be advised that these documents have not yet been reviewed for release and would be forwarded to the first-in,

first-out processing queue for Non-Personal Easy cases. The total number of pages for these four documents is 647, and your cost would be $97.05 (647 pages X $.15 per page). In addition, if you wish for us to conduct a thorough search for additional material that may be in our holdings in the Archives and Records Center, we estimate the costs to be $264.00. Fees are assessed in accordance with DoD Regulation 5400.7-R. Search fees are computed at $44.00 an hour.

Please be advised that your agreeing to incur these search fees will not necessarily result in the disclosure to you of all or any information you seek. If additional records are found which are responsive to your request, a detailed review to determine the releasability of the information would follow. It has been our experience that records responsive to your request may be classified or otherwise exempt from release in accordance with the exemption provisions of the FOIA. The application of these exemptions to NSA information has been consistently approved by the Federal Judiciary.

This is only an estimate. If, as we conduct the additional search, we determine that fees will be greater than the estimate, we will so notify you before continuing with our search. In addition, please be aware that an estimate for duplication fees is not included in the above amount because we cannot determine the number of pages to be released until the additional search has been conducted.

Please contact us within 30 days of the date of this letter to inform us if you wish to proceed further (i.e., have the four additional documents reviewed for release and/or have the additional search conducted). If we do not hear from you within that timeframe, we will assume that your request has been satisfied, and we will close it with no further processing.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (DJP4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Finally, you may be interested to know that some of the records concerning "SIGNIN" have been declassified and released to NARA. However, we are no longer the custodian of these records and, therefore, do not maintain copies of the records. To obtain the records, you will need to go directly to NARA. The address for NARA is: Director, Records Declassification Division

(NND), Room 6350, The National Archives at College Park, 8601 Adelphi Road, College Park, MD 20740-6001. The following chart may help you address your request to NARA:

ACCESSION #	DESCRIPTION
17143	Equipment Branch (Development Branch) History
13101	Correspondence on Miscellaneous US Comsec System
41249	Photographs: Equipment (WWII)
17461	Teletypewriter Key Generator System
17450	Plan for Service Testing of Teleconverter M-294
17448	Converter M-294 SIGNIN
17332	Signal Security Agency Development Branch Annual R
15215	Annual Report of Cryptographic Material Branch FY
15211	Description and Photographs of Cryptoequipment
14937	Cryptographic Plan (SIGIRA)

Additional information about conducting research at the NARA is available on the NARA Internet Website at http://www.nara.gov.

Sincerely,

for Marianne Stupar

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encl:
a/s

DOCID: 3486831

19

IV. B. 4

~~SECRET~~

THIS IS A COVER SHEET

BASIC SECURITY REQUIREMENTS ARE CONTAINED IN AR 380-35.

WARNING NOTICE:
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED.

NATIONAL SECURITY INFORMATION:
Unauthorized Disclosure subject to criminal sanctions

APPENDED DOCUMENTS CONTAIN SPECIAL INTELLIGENCE

(This cover sheet is unclassified when separated from classified documents.)

~~SECRET~~

IA Label 9
(1 Oct 78)

Edition of 1 Nov 73 may be used.

247388 f

TOP SECRET

ARMY SECURITY AGENCY

Washington, D. C.

THE ACHIEVEMENTS OF THE SIGNAL SECURITY AGENCY IN WORLD WAR II

Prepared
under the direction of
The Assistant Chief of Staff, G-2
WDGSS-14
February 20, 1946
TOP SECRET

TOP SECRET "ULTRA"

THE ACHIEVEMENTS OF THE SIGNAL SECURITY AGENCY IN WORLD WAR II

Contents

INTRODUCTION

With the cessation of hostilities in August 1945 the necessity for keeping secret many technological advances made by the Armed Forces during the conflict no longer existed and as a result extensive, if not complete, publicity could be given to them. Such, for example, were radar and the proximity fuse—the existence of the atomic bomb project had been inevitably revealed a little earlier by its devastating results at Hiroshima. Likewise, it has been possible to publish illustrated accounts of the spectacular successes of the Air Force; the less romantic but nonetheless essential contributions of the Service Forces have also been widely publicized. Throughout the War, moreover, the press was able from time to time to narrate the exploits of combat troops in action.

Yet, in the field of those Siamese twins, signal intelligence and communications security, no such publicity is possible, for by their very nature the hope of future successes is dependent upon the secrecy of past achievements. Here there is no point in time when one can say "now it can be told." On the other hand, if the Army in peace or in a future war is to make the most of the tremendous potentialities presented by these two aspects of a single problem, secret communications, it is necessary that our top leaders have an appreciation of the contributions made by the signal intelligence and communications security organizations during the War.

The ideal way of obtaining such an appreciation would have been a personal visit to Arlington Hall Station to note the war-time operations of the Signal Security Agency. By now, however, these operations have, of course, been greatly curtailed, and for this reason the present document has been prepared. It is hoped that the reader will gain from it some understanding of the problems faced by the Signal Security Agency, the general nature of the procedures and techniques used for their solution, the successes which were obtained, and the potentialities for the future.

W. PRESTON CORDERMAN
Brigadier General, USA
Chief, Army Security Agency

28 February 1946

THE ACHIEVEMENTS OF THE SIGNAL SECURITY AGENCY IN WORLD WAR II

I. BUILDING THE ORGANIZATION

The Signal Security Agency (SSA) owed its existence in World War II to the basic fact that valuable information may be derived by intercepting communications and reducing them to intelligible form. This fact has two aspects: efforts must be made to protect our own communications against examination by the enemy, while at the same time steps must be taken to derive as much information as possible from enemy communications. The SSA had primary responsibility for both these phases.

However logical this unification of responsibility in a single centralized organization now seems, it was achieved at only a relatively recent date. In World War I, for example, diversity, rather than unity, was the rule. Largely as the result of circumstances, it happened that so far as activity in Washington was concerned, the Military Intelligence Division conducted all work on compilation of codes and ciphers for use by American forces and also all solution of foreign codes and ciphers. In France, however, the corresponding organization in the AEF carried on only solution of German Army communications, leaving to the Signal Corps the task of compiling codes for combat purposes and the duties of interception and location of enemy radio stations by direction finding.

This separation of function continued for ten years after the War. Solution of current diplomatic traffic was performed by the Military Intelligence Division in a more or less clandestine unit maintained in New York, while the Chief Signal Officer supported another small unit in Washington engaged in the compilation of codes and ciphers for use in an eventual emergency. As a result of dissatisfaction caused not only by the division of responsibilities but also by a number of other concomitant factors, the functions of code compilation and of solution were united in 1930 under the Chief Signal Officer. This led to the establishment of the Signal Intelligence Service (SIS) which was essentially an amalgamation of existing units but began its work, so far as solution was concerned, with a change of emphasis: henceforth the SIS would be primarily concerned in peacetime with training of cryptanalysts for an emergency rather than with the solution of current diplomatic traffic. Though the need for training was acute, the abandonment of day-to-day solution of current systems had an unfortunate effect in interrupting cryptanalytic continuity, a point to which we shall return later.

In spite of greatly limited funds, the SIS was able in the years prior to World War II to lay securely the foundations upon which wartime expansion as the SSA was built. In 1934 the SIS took over from The Adjutant General

responsibility for printing, distributing, and accounting for cryptographic publications, and thus unification of operational responsibility for all phases of signal intelligence was at last reached. Staff supervision and coordination still remained, however, a responsibility of the Assistant Chief of Staff, G-2.

Activity of the SIS consisted of continuation of existing code production projects; establishment of a training program by which a small group of expert civilian cryptanalysts was produced, and another small group of officers, both Regular and Reserve, were trained in the varied phases of signal intelligence; development of intercept facilities to provide material for the cryptanalysts; and, toward the end of the period, the reestablishment, as a practical operation, of solution of current diplomatic traffic. In addition, time was found to do much planning for war and to carry on research and development in cryptographic and cryptanalytic techniques. All of this work was done by a very small staff: only seven persons from 1930 to 1936—by the outbreak of the War in Europe there were only nineteen.

Thereafter, a series of expansions resulted in the following strength on the day of the Pearl Harbor Attack:

Category	In Washington	In the Field	Total
Officers	44	1	45
Warrant Officers	0	0	0
Enlisted Men	28	149	177
Civilians	109	0	109
Total	181	150	331

Actual operating strength was somewhat less, since 22 of the civilians were still undergoing training and had as yet made no contribution to the work. A comparison of these figures with the strength of V-J Day (14 August 1945) will show the tremendous proportions reached by the wartime expansions:

Category	In Arlington	In the Field	Total
Officers	661	116	777
Warrant Officers	4	11	15
Enlisted Men	565	2139	2704
Enlisted Women	957	257	1214
Civilians	5661	0	5661
Total	7848	2523	10,371

These figures do not include, of course, the more than 17,000 officers and enlisted personnel engaged in signal intelligence activities under overseas theater commanders, nor do they give any adequate indication of the turnover of personnel in the Military District of Washington: by the end of the War more than 18,000 numbered badges had been issued to all categories of personnel at Arlington Hall (headquarters of the SSA) alone. To recruit such a staff and to maintain it despite the many influences which tended to dissipate and to lower strength were tasks requiring strenuous efforts.

The recruitment program was faced not only by obstacles which also beset other wartime agencies, such as the manpower shortage and the need for speed, but also by many problems peculiar to the SSA, most of the activities of which had no counterpart outside the Government from which to draw personnel. Many of its operations required persons of the highest intelligence, possessed of rare skills not easily definable, often demanding, as in the case of the language experts, years of study to produce proficiency. Messages in more than twenty-five languages had to be translated, yet in only a few instances were competent linguists easily obtainable. This problem was most acute in the case of Japanese, both because a knowledge of Japanese is rare in this country and because the volume of material to be translated was so great; it was also keenly felt in the case of languages like Finnish, Portuguese, and Turkish, where the volume was less but acceptable translators were rare indeed. The only recourse was to train personnel from the very beginning: ultimately, for example, 428 Japanese translators were trained in this way. The same method proved to be the only solution for supplying competent cryptanalysts: both by the use of training manuals in military cryptography and cryptanalysis and by apprentice training in operating units, the small number of competent cryptanalysts available in 1941 was gradually expanded, but the supply was never equal to the demand.

Moreover, the SSA was called upon to train large numbers of personnel for ultimate assignment to overseas units maintained by theater commanders. This training was given not only in formal courses designed to produce officers and men qualified in the various cryptographic and cryptanalytic specialties but also by participation in the day-to-day activity of operating units. Much was done also to coordinate training of signal intelligence and radio intelligence units being trained elsewhere in order to keep them abreast of the latest technical developments. In this connection it will be well to digress long enough to point out the trend exhibited during the War of breaking down the centralized authority of the SSA by setting up independent signal intelligence units under theater commanders. Such a change was motivated no doubt by a feeling that it would be necessary to maintain signal intelligence units close to military operations. Yet the experience of the War showed that modern electrical communications are so speedy that distance is no longer a factor that need be considered. Examples will be cited in the next chapter of messages transmitted many thousands of miles, promptly read and translated, and sent back to the proper commander in time for action.

Morale problems were particularly acute, for in addition to those encountered by other wartime agencies, involving living conditions, health, fatigue, and the like, the SSA had a number peculiar to itself. Chief among these was the mixed character of the personnel. Officers, enlisted personnel, and civilians worked side by side, and in each of these groups there were both men and women. A small unit composed of personnel from several of these groups might contain people having varying degrees of prestige and receiving different pay and privileges, yet performing exactly the same type of service (see Appendix, No. 1, a typical unit at work. Note that officers, enlisted

men and civilians of both sexes are here engaged on the same project). Moreover, there seemed to be no correlation between a category of personnel on the one hand and competence and achievement on the other. Brilliant work was done by individuals in all categories. Had it been possible to operate the SSA entirely with military personnel, or entirely with civilians, some friction might have been avoided, but an SSA made up only of military, or only of civilians, would have lost immeasurably the contributions of the other group. As it was, military personnel had to be stationed with the SSA for both operational and training purposes while having civilian employees made it possible to use the services of many not qualified for military duty.

Another factor not particularly conducive to the maintenance of high morale was the necessity of maintaining complete silence concerning every phase of one's work. Moreover, many of the operations involved nothing but drudgery and considerations of security prevented the individual employee in many cases from getting a clear understanding of how his or her work contributed to the war effort.

Continuous efforts were made to maintain morale at a high level by bettering conditions of work and furnishing employees with aid in the solution of their personal problems. While the rate of separations of civilian employees (4 per cent a month) seemed high, it was found to be actually lower than that of other comparable wartime agencies in Washington. Indeed, giving due consideration to the inherent difficulties, morale in the SSA was really high.

Early in the War space in the Munitions Building, where the SIS had been located from its founding, grew so crowded that larger quarters had to be secured elsewhere. At first it was expected that the SIS would be housed in the Pentagon, then nearing completion, but before such a move was effected, plans were laid for moving the SIS to a site of its own, preferably outside Washington. The SIS would thus have room for expansion, be relatively better protected from the danger of enemy bombing, and could maintain its security with greater ease if not forced to share a building with other War Department agencies.

The site ultimately chosen after examination of several possibilities was the premises of Arlington Hall Junior College in Arlington, Virginia. This location was close enough to the Pentagon, was not too far from the Eastern Primary Monitoring Station then being planned at Vint Hill Farms, near Warrenton, and in addition made possible the utilization of the housing facilities in the Washington area for quarters for personnel and dependents.

The property was acquired by court action for $650,000, with $40,000 additional for furnishings, and the War Department assumed possession on 14 June 1942. Arlington Hall Station was established as a Class IV installation under the Chief Signal Officer on 25 June 1942. Immediately units

of the SIS began to move into the former school building, now the Headquarters Building, Arlington Hall Station, and by 24 August 1942 all of the SIS was at Arlington Hall, the move having been consumated without interruption of operations.

Construction began almost immediately on projects designed to convert certain of the existing buildings to military purposes, and by September the program of new construction was in full swing. Besides many smaller buildings, two very large semi-permanent buildings were erected for operations. The first was completed in less than three months time; the second, erected in winter months, took a little longer, but after May 1943 all operating units were housed in the two operations buildings. Other construction provided barracks and mess halls for enlisted personnel, a station dispensary, theater, post exchange, and other service buildings; a motor pool, a fire house and warehouses. The final construction was completed by 1944: while many units have had to work in crowded conditions, adequate space was supplied for all operations. One of the important ancillary structures was a cafeteria, completed early in 1943 and enlarged in 1944, which ultimately provided service around the clock. At first the cafeteria was operated by the Welfare and Recreational Association of Public Buildings and Grounds, Inc., Washington, D. C., but its management was later taken over by the Post Exchange, which also operated branch exchanges and coffee bars in the operations buildings.

The Post was made secure by establishment of a guard detachment and the erection of a double steel fence provided with an alarm system. Another fence was erected around each operations building, entrance to which was limited to authorized personnel. Distinctive badges were issued to all categories of personnel and had to be worn at all times (see Appendix, No. 1). Access to the Post was forbidden to visitors except on official business, and efforts were constantly maintained to indoctrinate all personnel in the necessity of maintaining the physical and operational security of the Agency.

The SIS had been prior to the War a field service under the Chief Signal Officer. Though located physically in Washington, it was not a part of the Office of the Chief Signal Officer but was administered at first through its War Plans and Training Division and later through its Operations Branch. With the coming of war, however, reorganizations were made by the Chief Signal Officer which resulted in a series of changes of name. The old name of Signal Intelligence Service (SIS), which had existed since 1930, was abandoned for Signal Intelligence Division (SID), and, in rapid succession, this became the Signal Security Branch (SSB), the Signal Security Service (SSS), and, finally, on 1 July 1943, the Signal Security Agency (SSA), a name which remained unchanged until the cessation of hostilities. After the organization of the Army Communications Service within the Office of the Chief Signal Officer, the SIS-SSA, by whatever name it was called, was always a part of the Army Communications Service.

The need for enlisted personnel was met by increasing the strength of the Second Signal Service Battalion. This Battalion had been created as a company on 1 January 1939 to supply personnel for the various intercept stations then in existence. Later it furnished a convenient military unit to which enlisted personnel employed in the Military District of Washington

and elsewhere for other types of signal intelligence activity could be assigned. In November 1942 the post of Commanding Officer of the Battalion was united with that of Commanding Officer, Signal Security Agency: in this way it was possible to effect unified control of all SSA enlisted personnel wherever stationed. The Battalion had detachments not only at Arlington Hall Station but all over the world wherever it became desirable to conduct any intercept activity. The Battalion did not, of course, include signal intelligence personnel directly under the control of theater commanders. While the Battalion embodied many unorthodox features—its maximum strength, for example, surpassed 5,000 officers and men and at the end of the War it was commanded by a Brigadier General—it effectively solved the problem of how to administer the amazingly complex activities performed by enlisted personnel working for the SSA.

Throughout the War—indeed, since 1861—the activities carried on by the SSA were closely associated with the Signal Corps. A glance at the Appendix, No. 2, a historical outline of how the United States Army administered its code and cipher work from 1861 to the present, will clearly show that while at times other Army organizations made outstanding contributions to the work, in the main this work was a responsibility of the Signal Corps. Yet from 1917 on, if not before, this work was also of the deepest interest to G-2, and in World War I the greater contributions were, in fact, made by the Military Intelligence Division. This reflects the essentially dual nature of the problem. That phase of the activity of the SSA which concerned the production of intelligence was chiefly of interest to G-2, yet could be carried on solely with the contribution of the Signal Corps in the development of intercept facilities. On the other hand the efforts of the SSA to preserve security of our own communications, a matter over which G-2 exercised supervision also, required closest association with the Signal Corps. Indeed, signal intelligence activities can be effectively carried on only when there is the closest liaison with signal security activities.

It has already been noted that the SSA was administratively and functionally a part of the Signal Corps, but G-2 exercised staff supervision and control. While channels were created whereby G-2 could exercise this control without at every step going through the Office of the Chief Signal Officer, nevertheless the SSA was primarily a Signal Corps agency, its personnel were Signal Corps employees, and for purposes of supply it relied on Signal Corps facilities.

Since it was increasingly felt by G-2 that the SSA was the most important source of intelligence, even closer control was required and therefore, on 10 December 1944, there came a change. The SSA was removed from the Signal Corps for operational control, which was now assumed by G-2, but administrative control was still retained by the Signal Corps. This cleavage of control was by no means clearcut and sharply defined: the line of division was not straight, since the organization was pragmatic rather than theoretical, but in the main the differentiation thereafter was operational control exercised by G-2, administrative control maintained by the Signal Corps.

Divided control, such as this was, however, proved far from satisfactory in practice and was ended on 15 September 1945 by transfer of administrative control also to G-2, with the change of name from Signal Security Agency to Army Security Agency (ASA). This had the effect of associating the organization more closely with G-2, the user of one of the two chief products, but it will necessitate that in the future liaison be constantly maintained with the Signal Corps so that not only an adequate supply of trained personnel may be available for the communications side of its activity but also the increasingly closer relationship between signal intelligence and signal security may be maintained by the closest cooperation. Moreover, it also resulted in once more consolidating all responsibility for signal intelligence and signal security in a single organization, since the units formerly under the control of theater commanders were now made a part of the ASA.

As will be abundantly clear from specific references in the two following chapters, the SSA had the incalculable advantage of collaboration with the corresponding units of the United States Navy (OP-20-G and OP-20-K). Liaison with the Navy had long been in progress before the War but throughout the conflict it constantly increased in both the cryptographic and cryptanalytic fields. For some years before the War the Army and the Navy had been collaborating in the cryptanalytic attack upon diplomatic traffic, but the Office of Naval Communications, being pressed for personnel and facilities needed by units at work on enemy traffic of a purely naval character, asked the SIS to take over more and more work on diplomatic traffic until in the summer of 1942 the Army alone had full responsibility for work on diplomatic traffic.

Equally profitable was the collaboration with the British Government Code and Cypher School (GCCS), an organization which had maintained cryptanalytic continuity since 1914 and was prepared to make great contributions of information concerning foreign cryptographic systems under study. The need for continuity was so important that it is doubtful whether success in solution of certain diplomatic systems could have been achieved in time to be useful, had not the British supplied the necessary information not available here, owing to the break in continuity which, as we have seen, took place in 1930. While it is true, as will be described in Chapter II, that the cryptanalysts of the SIS had before the War solved the most secret Japanese diplomatic system without any British aid, this achievement could not have been reached except for the fact that for some years prior to this time Japanese traffic had been under constant study and the cryptanalysts had information available covering the whole period 1921-1939. The gathering of this information had, however, taken the best part of eight years: it is usually futile, nowadays, without the necessary continuity of background information, to begin cryptanalysis of the communications of any large government and hope for considerable success at once. The debt of the SSA to GCCS in shortening the period between the beginning of study and the production of translations was in the case of the diplomatic traffic of certain governments very great indeed.

This collaboration with the British began with the implementation of basic War Department decisions, reached in August 1940, to exchange information

with them. Early in the next year the first SIS mission was sent to England to establish the basis for liaison and in the summer the SIS and GCCS first exchanged permanent liaison officers, a relationship ever since maintained. Special missions have, however, also been sent and received from time to time. Intercommunications by radio, cable, and mail, have been constantly maintained. Frequent agreements have been made to avoid unnecessary duplication of effort: the chief of these was reached in 1943 whereby the British assumed primary responsibility for signal intelligence operations for the War in Europe, the SSA, for those for the War in the Pacific, though neither Agency abandoned work in the field of the other's responsibility. This exchange of information has been broadest in cryptanalytic activity: considerations of security have limited cooperation in cryptographic compilation and development to work on systems used in combined British and American operations. A similar profitable collaboration has also been conducted, though to a much more limited extent, with the Examination Unit (XU) maintained by the Canadian Government in Ottawa, and with the Wireless Experimental Center (WEC), maintained by the Indian Government at New Delhi.

The SSA provided trained personnel for and collaborated with U. S. Army Signal Intelligence Services in all theaters: Mediterrean Theater of Operations, European Theater of Operations, Southwest Pacific Area, China-Burma-India Theater, Central Pacific Area, etc. Collaboration between the SSA and the Central Bureau, Brisbane (CBB), began with the founding of the latter organization by joint action of the Royal Australian Army and the United States Army in the spring of 1942. As will be later seen, this cooperative effort was maintained by constant intercommunication, particularly in the case of the Japanese Army cryptanalytic problem.

From time to time the SSA has received from the users of its products letters of commendation for its activity. The most striking comment of this kind came, however, not in a direct communication to this Agency, but in the published text of a letter from General George C. Marshall, then Chief of Staff, to Governor Thomas E. Dewey of New York, dated 25 September 1944. Reference will be made again to this letter, the full text of which as it appeared in The New York Times is reproduced in the Appendix, No. 4.

II. THE PRODUCTION OF INFORMATION

Modern intelligence services are able to derive information useful for military purposes from many sources, but the most fruitful and most authentic is the enemy's message traffic and the communication system over which it is transmitted. Indeed, though messages differ in value, experience has proved that there are no messages, no matter how insignificant in content, which have potentially no intelligence value. Therefore, the cryptanalytic attack had to be made not only upon the purely military traffic transmitted by enemy forces but also upon diplomatic, commercial, and private messages as well. Even plain-text messages could not be neglected, but the largest part of the intercepted traffic was, of course, in cryptographic form and required cryptanalytic treatment before it could be read.

While some of the techniques used by the SSA were not strictly cryptanalytic in character, e. g. traffic analysis, secret ink solution, and exploitation of telephonic communications, the production of information involved, in general, the following steps:

a. Interception of traffic in large volume;
b. Traffic analysis of intercepted messages;
c. Solution of the cryptographic systems used;
d. Decryptographing of messages sent in solved or partially solved systems;
e. Translation of such texts as were in foreign languages, and
f. Publication of the texts in a form useful to the Military Intelligence Service.

A figure in the Appendix (No. 3) illustrates the various steps by which an enemy message passes from its originator to MIS. (Note that interception has been here represented by the artist as being performed by a mobile unit in a truck: many of the intercept missions were, of course, performed by fixed installations.)

A. INTERCEPTION

No cryptanalytic attack upon the communications of a foreign government can hope to be successful unless an adequate supply of intercepted material is available for study; nor can proper measures for safeguarding our own communications be taken without constant monitoring of the traffic sent out by American stations. It therefore became necessary to establish facilities for the interception of radio traffic in large volume.

Prior to the war there were seven fixed intercept stations located as follows:

No. 1 Fort Hancock, New Jersey
No. 2 Presidio of San Francisco, California
No. 3 Fort Sam Houston, Texas
No. 4 Corozal, Panama Canal Zone

No. 5 Fort Shafter, Territory of Hawaii
No. 6 Fort McKinley, Philippine Islands
No. 7 Fort Hunt, Virginia

Constant efforts during the War expanded these facilities greatly. In the end there were eleven fixed stations, many of which were far larger than any operating in 1941. These eleven, which were found sufficient to supply the necessary volume of traffic, were distributed as follows:

No. 1 Vint Hill Farms, Warrenton, Virginia
No. 2 Two Rock Ranch, Petaluma, California
No. 3 Indian Creek Station, Miami Beach, Florida
No. 4 Asmara, Eritrea
No. 5 Fort Shafter, Territory of Hawaii
No. 6 Amchitka, Aleutian Islands
No. 7 Fairbanks, Alaska
No. 8 New Delhi, India
No. 9 Bellmore, Long Island
No. 10 Tarsana, California
No. 11 Guam

The three largest stations (at Vint Hill, Two Rock, and Fort Shafter) were equipped with elaborate arrays of high-directivity antennas for all-round coverage. These stations had been located so as to make easy the electrical forwarding of the intercepted traffic to Arlington Hall and the largest portion possible of intercept missions was assigned to them. The supplementary stations, particularly those at Asmara, Amchitka, Fairbanks, and New Delhi were located so as to intercept signals which could not be copied at the larger stations, and in general they had antenna systems beamed at specific targets or sectors. The stations at Bellmore and Tarsana were assigned the task of monitoring United States traffic for security purposes. Considerable assistance was rendered to the intercept facilities of the SSA, particularly in the period before the SSA's own intercept facilities were fully developed, by radio intelligence companies stationed on the West Coast and in the Pacific Area.

Among the new items of equipment developed during the War for use at intercept stations were "multicouplers," which allow the signal from one antenna to be coupled to several receivers; a "Hellschreiber Facsimile Recorder," for copying signals of this German system; and a "Time Delay Device," which accomplished a delay of from three to ten seconds between the time a signal is received and the time it is necessary to copy it, making it possible to start a recorder to take down the entire transmission for later transcription.

Intercept activity was coordinated and controlled by staff units at Arlington Hall which supplied the stations with technical advice. Speedy transmission from the intercept stations was effected chiefly by special teletype lines, which came more and more to take precedence over other means such as cable and air mail. From four teletype lines in operation on 7 December 1941, the number of such lines grew until on V-J Day there were forty-six. The amount of money paid for monthly rental of land-line teletype facilities alone reached in August 1945 the large sum of $58,918.02 but this figure does not include the cost of radio-teletype facilities, paid for

by the Army Communications Service, for which no data are available to the SSA. Average monthly volume also constantly grew:

February 1943	46,865 messages
December 1943	279,034 messages
July 1945	381,590 messages
August 1945	289,802 messages

Arrangements were also made for obtaining traffic from radio intelligence units operating in theaters of war; from the Navy; from the several offices of the Chief Cable Censor; and from British cooperating centers.

B. Traffic Analysis

Traffic analysis, a procedure which first arose from attempts to reconstruct enemy communications networks and their characteristics with the aim of improving intercept facilities, became highly useful also for two other purposes: (1) through study of the external features of the message as distinct from the text itself, together with direction finding, by which it is possible to locate the sites of unknown radio stations, traffic analysts were able to provide cryptanalysts with much useful information not otherwise obtainable; and (2) statistical study of the fluctuations in the volume of traffic passing in each circuit, and inferences drawn therefrom, became an important source of military intelligence. Traffic analysis can be carried on, of course, independently of successful cryptanalysis: useful information can be derived by traffic analysis even before a message is readable, but when the two techniques are combined, each is aided by the other.

While traffic analysis had been used to a limited extent in World War I, the British were the first to develop the science extensively in World War II. The beginnings of traffic analysis in the SIS date from April 1942. A mission was sent to England to gather information and upon its return it was possible to set up traffic analysis as an integral part of the SIS. As a result of this mission, efforts of the SSA in traffic analysis were to be concentrated on traffic in the Pacific theater, leaving to GCCS the primary responsibility for that in the European, a logical arrangement arising from geographical considerations.

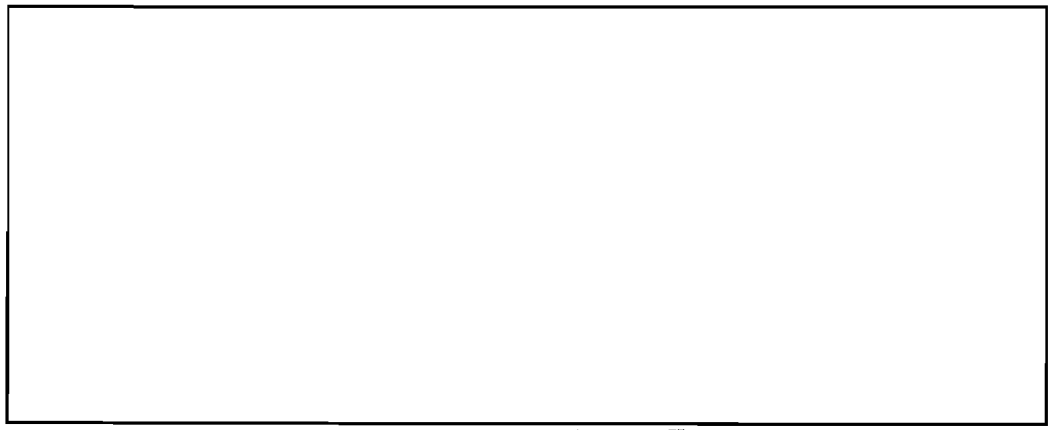
The initial problem in traffic analysis for the SSA was the solution of the code numbers used to indicate message-center place names occurring in Japanese military messages, and the first success was achieved in September 1942. By the following June nearly all of the twelve main systems had been reconstructed, permitting accurate location and mapping of radio stations and circuits. Four distinct major military networks were identified, those used by the Imperial GHQ in Tokyo, the Southern Field Force, the Water Transport organization, and the Army Air Force. The adequacy of the techniques used was proved when, on 1 April 1944, the Japanese introduced a completely new place-name code which was almost wholly solved within a month, about half of the names being identified within 48 hours. Technical assistance given the intercept stations was responsible, at least in part, for the rapid increase in volume of Japanese military intercepts.

Contributions of traffic analysis to military intelligence began with the location of military message centers attached to unit headquarters. The identification of nets and unit organization revealed troop locations and chains of command, thus giving highly important information concerning the Japanese Order of Battle. Traffic flow analysis—the study of variations in traffic volume and patterns of station activity—gave indications of impending enemy activity. Convoys were detected and followed merely by studying the changes in the pattern of communications in the Water Transport code between various seaports along the route. Analogous studies of patterns in Air Force and Army Administrative codes led to detection of aircraft and troop movements. Analysis of communications between field units and their home depots indicated the location of almost all divisions south of Manchuria. The movement of a unit in the field could be detected from its home depot traffic, or through readdressed messages, or by messages addressed to the unit code name in lieu of a specific message-center location. Finally insight into the general content of diverse classes of messages, gained through traffic analysis, aided in establishing priorities in handling the thousands of messages received daily. Though publication of daily and weekly traffic analysis bulletins began in September 1942, the greatest emphasis on the intelligence aspect of traffic analysis came in late 1944 and 1945. Where deceptive measures are not employed, traffic analysis can yield a very large amount of fairly reliable intelligence; where deception is effectively practiced, deductions from traffic analysis must be used with extreme care. Since, however, there was currently no evidence that the Japanese engaged in deceptive communication measures (a fact which was confirmed after V-J Day), valuable results from traffic analysis were frequently obtained.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

C. Cryptanalysis

Cryptanalytic procedures are never stereotyped and permit no easy description. Methods must be worked out to suit individual cases, but, in general, the following steps usually take place in one order or another.



too much emphasis cannot be placed upon the need for cryptanalytic continuity, a topic which has also been mentioned previously in connection with the collaboration of the British (see page 9). It is characteristic of most cryptographers that they tend to introduce new cryptographic features and elements in a conservative manner. Thus, a new system will frequently not represent a radical departure from its predecessor but will, rather, be merely a refinement and improvement of what went before. Since this is likely to be so, the cryptanalyst who can start his study of a new system with a good acquaintance with the cryptographic character of the one just made obsolete, and of others used concurrently by the same government, will be at a great advantage. The basic factor underlying all successful cryptanalysis, however, is constant watchfulness for significant details which may provide an entry: one or another of the operations mentioned above may reveal the nature of the system but the surest method is statistical analysis.

In World War I and for many years thereafter, such statistical analysis was dependent upon hand methods alone. The cryptanalyst or his clerical assistants were forced to make frequency counts or other statistical tabulations of the units of text (letters or digits), taken either singly or in groups, by hand. Not only did the process involve an immense amount of drudgery but it was also easily subject to serious error. The eye had to keep the place in a meaningless text while the hand made the necessary indications on the charts. Naturally, the work, to be dependable, had to be painstakingly accurate: the result was that it was time-consuming. Even under the conditions of World War I, when the volume of intercepted traffic was relatively low, this was already a problem of most serious proportions. As a consequence, steps were taken during the period of peace to find adequate solutions to the problem. The most significant trend in cryptanalytic research and development during World War II has been, in fact, the extent to which machinery has been used to speed up hand methods and also to perform operations which, because of their magnitude, could never have been attempted without such apparatus.

A very large measure of the success of the SSA in cryptanalysis must be attributed directly to this fact. The enormous increase in the volume of intercepted traffic would alone have made hand methods wholly inadequate to accomplish the task set us in this War. Fortunately, none of the enemy nations seems to have realized the possibility of developing such machinery and the necessity of protecting their cryptographic systems against attack by such means, or if they did, as was true in the case of the Germans, the realization was not too clear and insufficient emphasis was placed upon the development of mechanical and electrical analytical equipment. The SSA, on the other hand, has had to keep constantly in mind, while developing cryptographic systems for our own use (see Chapter III), the possibility that other nations might also make, during the War or later, similar advances in machine cryptanalytic techniques and to prepare against that contingency. Thus, any new development in cryptanalytic techniques has the immediate effect of causing a converse development in cryptographic techniques, and vice versa. This is the fundamental reason why all research

and development in both fields must be carried on within a single organization.

Several types of machinery have been used. The first of these is standard tabulating machinery, including machines available on the open market as well as machinery of the same general type modified or developed expressly for the SSA. The method involves the recording of data on a card in which holes are punched by means of a key-punch machine and the processing of decks of such cards by a number of other machines.

While few, if any, cryptanalytic units have failed to make extensive use of these machines, by far the greatest employment of them has been in the solution of the Japanese Army systems. Indeed, the solution and processing of any significant quantity of the hundreds of thousands of messages in those systems would have been impossible without these machines. An indication of the growth of the use of tabulating machines of this type by the SSA is the fact that whereas only 13 machines and 21 operators were at work at the outbreak of the War, 407 machines had been installed at the peak in April-May 1945, involving a total of 1275 persons as operators and supervisors. The monthly rental for these machines reached a peak in June 1945 of $60,982.

In addition to standard and specialized tabulating machinery, another important category of machines was that generally referred to as Rapid Analytical Machinery (RAM). Machines of this category usually employ vacuum tubes, relays, electronic circuits, and photoelectrical principles. A number of different types, designed within the SSA for specific operations, were developed and constructed by the SSA itself or in cooperation with several contractors, and set up at Arlington Hall Station. One cryptanalytic machine costing almost a million dollars, was basically homologous to an automatic telephone exchange capable of serving a city of about 18,000 subscribers and the SSA had two such machines. These two machines were capable of performing operations which, if done by hand methods, would have required over 200,000 people. A second cryptanalytic machine, specifically designed to perform a certain type of test by means of electrical relays, served as the equivalent of 6,000 cryptanalysts; and an improved machine of the same general nature but using vacuum tubes and electronic principles rather than relays, is now almost completed. It is expected to operate at least 500 times faster than the relay type and can be estimated to be equivalent to having 3,000,000 people at work. In the development and construction of these highly specialized cryptanalytic machines the SSA expanded several million dollars but it could hardly have operated without them.

D. Solutions

Cryptographic systems have grown in complexity very greatly since World War I, and in a brief report such as this it is impossible to give

General Marshall, in his now famous first letter to Governor Dewey, dated 25 September 1944, and disclosed in The Joint Congressional Hearing in the Pearl Harbor disaster, stated that "our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government." (For the full text of both letters, see the Appendix, No. 4.)

In addition to this machine, which remained in current use until the end of the War because knowledge of its solution was fortunately kept secret during the War, the Japanese also began to use for diplomatic purposes a variety of other high-security systems based on intricate cryptographic principles. The system used for the communications of the Japanese military attachés, for example, provided for encoding the message by means of a two-part code; the code message would then be further protected by enciphering the code message by an extremely secure cipher method. In addition, the key indicators and message numbers were also disguised. Moreover, the various cryptographic elements (code book, key book, and so forth) were changed at irregular intervals. The result was that the best efforts of a large staff of the ablest experts working continuously on this problem were necessary to solve the diplomatic and military attaché systems. Solution was, even so, effected in nearly all cases, providing a very large volume of translated messages giving significant information as to the intentions of the Japanese, conditions in the Far East, and also of conditions in Europe. Indeed, it has been said that the Japanese military attachés were the best secret agents of the United Nations on conditions inside occupied Europe.

The value of the intercepted Japanese diplomatic and military attaché traffic for intelligence purposes can best be illustrated by representative translations, but of the many thousands of messages which appeared in the SSA Bulletin, only a few can be chosen for inclusion in a brief report such as this. Full texts of four characteristic messages appear in the Appendix as follows:

a. Berlin to Tokyo, serial number 878, parts 14-17 inclusive, SSA Bulletin No. B-3348, 9 November 1943, translated 4 December 1943, sent in the JAS (military attaché system). The message from which this sample is taken consisted of 32 parts, all of which were ultimately translated. The full text, too long for reproduction here, is a report of a visit made in the fall of 1943 by a subordinate of Baron Oshima to the German western fortifications. The military information contained in this message was of incalculable advantage to the planning of the invasion of France. See Appendix, No. 5.

b. Berlin (Oshima) to Tokyo, serial number 968, parts 1-3, SSA Bulletin No. B-13420, 10 August 1944, translated 12 August 1944, sent in the JAD (diplomatic) system. This message, here reproduced in full, has been described by officers

more than an inkling of the length to which many foreign governments have gone in improving their methods. Larger and more scientifically constructed codes were introduced; complex radio procedures and superencipherment systems were added; and intricate cipher machines were developed. By the year 1939, when the outbreak of war in Europe caused the first substantial expansion of the SIS since 1930, cryptanalytical attack was being centered, in accordance with directives from G-2, upon the diplomatic communications of four governments only: Japan, Germany, Italy, and Mexico, work having been begun in that order. The group assigned to Mexican systems, however, expanded its activity early in 1941 to include systems used by several other governments, both in the Eastern and Western Hemisphere, specifically those of France, Spain, Portugal, Brazil, and a few Spanish-American countries. As noted above, all systems thus far studied were entirely diplomatic in character; indeed, little traffic of other categories was then being intercepted. Work proceeded along these lines, effecting solutions which will be discussed in greater detail a little later, but so far as cryptanalysis is concerned, this was the situation existing on the day of the Pearl Harbor attack. By the end of the War cryptanalytic attack had been directed against the cryptographic systems of every government which uses them except only our two Allies, the British and the Soviet Union.

(1) Japanese Diplomatic and Military Attaché Traffic

The first diplomatic systems to receive attention in the SIS were the Japanese, and from 1933 to 1941 eleven such systems were studied and solved. For the most part they were not greatly advanced in cryptography from those solved before 1930, but in two machine ciphers, the earlier of which had appeared by 1932, the Japanese demonstrated that they had read with profit The American Black Chamber, in which Herbert O. Yardley, formerly an officer of the Military Intelligence Division, indiscreetly revealed to the world American successes in solving foreign cryptographic systems.

The machine ciphers presented cryptanalytic problems of greater difficulty, involving not only the reconstruction of a complicated machine but also thereafter the day-to-day recovery of a great number of keys. The second of these machines, introduced in 1938, was much more complex than the first and required almost two years of concentrated study to solve; its solution by the SSA, unassisted by any other cryptanalytic organization, represented an achievement of first magnitude and importance. It is now known that the German organizations attempted the feat and failed, as did the very competent British organization. It was in February of 1941 that an SSA cryptanalytic mission to London presented the British with the details of the solution together with a machine, constructed for the purpose, to facilitate the decipherment of messages. The remarkable feature of this solution was that a machine capable of deciphering the Japanese messages was reconstructed wholly by analysis: the SSA has never seen one of the Japanese machines. The importance of this solution can hardly be over-estimated.

in MIS as "worth all the expenses of maintaining the SSA." The text describes conversations with the head of the Todt organization, Albert Speer, in which the latter revealed to the Japanese, and, thus to us, highly important information concerning the production of munitions in Germany. See Appendix, No. 6.

c. Hanoi to Tokyo, no serial number, SSA Bulletin No. H-164499, 22 January 1945, translated 1 February 1945, sent in the JBB (diplomatic) system. This message is important because it reveals that the Japanese were interested in obtaining uranium. See Appendix, No. 7.

d. Moscow (Sato) to Tokyo, serial number 1476, SSA Bulletin No. Spec. (Tl, 29 July 1945, translated 30 July 1945, sent in the JAA-2-JAJ (diplomatic) systems. This three-part message, the translation of which was available to President Truman during the Potsdam Conference, reveals the activity of Sato, Japanese Ambassador to Moscow, at the time of the conference. See Appendix, No. 8.

It will have been noted that while two of these four messages were translated within two days after they were transmitted, another took about ten days and the fourth nearly a month for translation. Delays of this kind may be attributed to a number of factors. In the first place it frequently happens that a cryptographic system is of such a complex nature that a considerable volume of traffic must be available before successful cryptanalysis can be initiated. Hence when only a single or even a few messages have been intercepted it may still require several days or even weeks to elapse before there is sufficient traffic available in the same key to permit solution. Secondly, a sharp rise in the volume of intercepts may create a backlog of unprocessed messages which may take several days to eliminate. Thirdly, there is the question of translation: in the case of Japanese texts, for example, in spite of the great efforts made to train competent Japanese translators there never were enough of these to keep up at all times with the production of the cryptanalysts. To prevent highly important messages containing information demanding immediate action by MIS from being laid aside until the information was too late to be useful, a policy was adopted of scanning the messages as they became readable in order to sort them according to the degree of urgency. In spite of these difficulties, however, it frequently happened that messages were intercepted, decoded, translated, and placed in the hands of MIS before their addressees might be presumed to have read them. A conspicuous instance of this kind was the famous message by which the Japanese transmitted through the Swiss Government their intention to accept the surrender terms. The fact that the Japanese had accepted the Allied terms was known in the MIS several hours before the Swiss Minister was able to give the message to the State Department.

(2) Japanese Army and Air Force Traffic

The following paragraph is quoted from a communiqué which appeared in The New York Times on 4 September 1943:

> Wewak: Our strongly escorted medium bombers attacked an enemy convoy of five cargo ships and two destroyers which arrived during the night with reinforcements and supplies for the enemy garrison. Coming in at masthead height, our bombers scored direct hits with 1,000-pound bombs on three freight transports, each of 7,000 tons, sinking them. In addition, one of the escorting warships and a 1,000-ton cargo ship sustained direct hits and were left ablaze. Numerous small harbor craft were destroyed by strafing. Intense anti-aircraft barrages were encountered and barrage balloons from ship and shore were employed in an endeavor to halt our low-level attacks. Thirty-five fighters flown in from the rear bases to protect the convoy were intercepted in the air. Twelve of these were downed with eight others probably destroyed and five damaged. Three of our bombers and one fighter were lost.

Note that in the entire communiqué there is no explanation of the method by which the American commander in the New Guinea area learned of the presence of the convoy at Wewak: the impression is given, as indeed was intended, that the good fortune of the bombing mission in finding the convoy solely was the result of chance. Yet this was not so. A message had been intercepted and read by the SSA (on 20 August, nearly two weeks ahead of time) which foretold to the Japanese at Wewak the arrival there of the convoy on the first or second: for the full text as translated, see the Appendix, No. 9. The message in its English form was forwarded speedily to MIS and thence by radio to the proper commander for his use. This instance is, of course, only one of many which could be adduced to show how in an age of radio communications the necessity of forwarding an intercepted text thousands of miles to a control agency for decipherment and its return when made readable causes little more delay than would have taken place had the cryptanalysts been at work at the points of interception.

In order to prevent the Japanese commander at Wewak from suspecting the truth, precautions were taken, in accordance with rigid regulations, to provide an additional source of the information which he would naturally suppose to be the only one, namely, reconnaissance planes were sent over Wewak. On many occasions, in fact, American commanders were in possession of valuable information provided by the SSA which they could not use because to do so would have run the risk of revealing to the Japanese the fact that their secret communications were being read by us. The ability to continue reading the traffic as a whole was often a military objective of greater importance than that involved in the successful completion of a specific mission.

The bombing of the convoy at Wewak, as just described, is a good example of the effect of the translation of an isolated message—only the third part of a three-part message had been translated in time—but many messages, which individually are less striking, when taken together and coordinated by MIS, permit the accomplishment of even more spectacular results. The following paragraph is taken from a memorandum prepared by an officer in MIS (27 March 1945):

Use of Ultra [= SSA] Information for Attack on Japanese Troop Convoy

1. Information received. Ultra traffic on and shortly after 2 April 1944 revealed Japanese plans to send a large convoy, designated as the "TAKE" Convoy, to Halmahera and New Guinea. The convoy, consisting of nine merchant vessels and about twelve escorts, sailed from Shanghai for the south in the latter part of April, carrying 12,874 troops of the 32nd Division, about 8,170 troops of the 35th Division, with equipment and other military supplies. Messages furnished the identity of the ships and full details about the troops and cargo loaded on each ship. Traffic analysis disclosed the approximate date the convoy was scheduled to leave Shanghai for Manila and provided current information on the convoy's approximate position on its trip from Shanghai to Manila. Before the departure from Manila on 1 May, messages revealed the following information:

a. scheduled noon positions for each day from 2 May to 9 May;

b. an outline of an alternate route to be followed only on receipt of special instructions;

c. a plan to divide the convoy into two groups on 7 May to a point N of Halmahera, one part (presumably the 35th Division ships) scheduled to go on to Manokwari, and the other part presumably (32nd Division ships) scheduled to go on to Wasile on Halmahera.

2. Action taken. Information on the composition, loadings, movements of the TAKE Convoy was forwarded to the appropriate field commands, as it became available.

3. Operational results. On 26 April the convoy was attacked by submarine at a point 30 n. W of Lanag (NW Luzon) and one ship was sunk. On 6 May the convoy was again attacked by submarine 100 n. NW of Menado and three additional ships were sunk. About 4,000 troops together with ordnance and other supplies were lost as a result of those sinkings, including the Commanding Officer and 2,700 troops (substantially all) of the 220th Infantry Regiment of the 35th Division. Two Japanese divisions, both critically needed as reinforcements, were thus decimated and their effectiveness seriously reduced. Both divisions have since been met in combat. The above information concerning operational results also was received from Ultra sources.

4. Ultra material used. Preparation of the intelligence dispatched to the field commands required the examination and integration of a large number of separate and frequently fragmentary messages and traffic analysis.

The fact that the two examples already chosen were both concerned with the sinking of convoys should not be allowed to give the impression that this was the only phase in which intelligence was derived from Japanese Army messages. To quote again from the report already cited as prepared by an MIS officer:

> A 28 May [1944] message, available 1 June, mentioned supplies needed by the 18th [Japanese] Army (controlling operations in eastern New Guinea) which must arrive at Wewak by the end of June in order to be of use in "the attack on Aitape." In a 24 June message, available shortly thereafter, the Southern Army stated that the 18th Army would attack Aitape. Various other fragmentary messages, all showing that an attack on Aitape was planned, were also received. On 25 June there became available a 20 June message from the 18th Army reporting that it was planning an all-out attack against the U.S. Aitape perimeter, to begin about 10 July and giving the detailed dispositions of each division under the command of the Army, plus the planned operations of each division in the attack. Total strength of the forces involved was stated in the message to be about 20,000 . . . . All of [this] information was made available to the Commander-in-Chief, Southwest Pacific Area, before the date of the planned attack. . . .The Japanese attack was made on schedule and was completely defeated with heavy losses to the Japanese.

The resulting U. S. action was reported by The New York Times in three communiqués, as follows:

> Advanced Allied Headquarters on New Guinea: July 12 Communiqué: Aitape-Wewak: our medium units attack planes and fighters with twenty tons harassed enemy-occupied coastal sectors from Wewak to Yakamul, starting fires in bivouac and supply areas. Air and naval patrols attacked lines of communications.
>
> July 13 Communiqué: 45,000 Japanese troops trapped between Aitape and Wewak on New Guinea since April have started a desperate battle to fight their way to the northern part of the island.
>
> July 14 Communiqué: Our outposts inflicted heavy casualties in a preliminary engagement with an enemy force moving westward, apparently to attack our Aitape position. Our medium units and attack planes with 53 tons of explosives, struck enemy concentrations in the Yakamul and Wewak areas.

The examples just given show how the product of the Japanese Army cryptanalytic projects was of the greatest value in military operations in the Pacific area. We must now turn to the steps by which the product was made possible. Before the War attempts by the SIS to solve the secret communications

systems of the Japanese Army had, for lack of sufficient traffic and cryptanalytic personnel, been fruitless. In the summer of 1941 the British made available a fair amount of traffic and the results of investigations of this material carried on by them in the Far East. Some success had been achieved, but the Japanese had, by introducing certain changes, thrown the British off the tracks: current material was no longer readable. Immediately after the attack on Pearl Harbor more SIS personnel were assigned to the Japanese Army problems, but little could be done except to sort and file the traffic. Thus, cryptanalytic continuity was broken for a time.

[redacted]

compared roughly to the operation of demolishing a building by undermining its substructure and causing the building to collapse suddenly; code solution is more like a mining operation, the ore is taken out of the mine bit by bit.

By the autumn of 1942, however, traffic sources had been established and more personnel had been obtained, so that considerable attention could be given to these problems. The method of attack which seemed most likely to prove successful was that of going back to the last period of British solution and attempting to work forward, step by step, to current periods; in other words, to provide cryptanalytic continuity. This historical method, though seemingly a long way round, was really the only recourse, and it was

fully justified by the results. By January 1943 progress had been made beyond the period of British success, and at the same time encouraging results were being achieved in the recovery of code groups for addresses, which had previously seemed so hopeless a problem that outstanding British cryptanalysts had counseled dropping the study. In April 1943 the first break into a current system (that used by the Japanese Army Water Transport organization) was made possible as the result of a mistaken notion on the part of the Japanese that so much security was provided in their current system that a much smaller number of keys was adequate for the encipherment of the indicators. In this instance the entering wedge was simultaneously discovered (almost in the very same hour) by personnel of the SSA at Arlington Hall and of the CSB in Australia. It was most successfully exploited as the result of the constant collaboration maintained by daily intercommunication between the two organizations.

The result of this initial solution was a reorganization of facilities within the SSA leading to considerable expansion in personnel and services devoted to the Japanese Army problem. Ultimately, the number at work on these problems exceeded that of personnel at work on all other cryptanalytic problems combined, and yet there never were enough trained workers to carry out fully all phases which needed to be done: the man-power situation was such at the time that the demand for personnel was always greater than the supply, and even when the needs were temporarily filled there always was some delay between the time new personnel reported for duty and the time they were ready to participate effectively in actual operations, because preliminary training was usually essential.

By early June 1943, two months after the initial break into the system, translation of Water Transport messages were being forwarded to MI3. Thereafter, until almost the end of the War, the Water Transport system provided not only a broad picture of the Japanese Army shipping organization and activities but also, from time to time, information regarding specific operational movements of which the logistics problems were discussed in Water Transport messages. To quote once more from General Marshall's letter to Governor Dewey:

> "Operations in the Pacific are largely guided by the information we obtained of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys. The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point. The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based on timing of the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks."

Although undoubtedly General Marshall included in this tribute to the signal intelligence services the very outstanding contribution from the signal intelligence service of the Navy, for fleet movements are mentioned, the bulk, however, of the information of the type cited came from the SSA.

Solution of the main Ground system was effected by a series of discoveries that began in May 1943 and culminated in decipherment of messages in September of that year. Also, by the summer of 1943, solution of the address system had reached a point where the addresses of current intercepts were readable. Reconstruction of the address code books, which had hitherto been carried on exclusively by a British organization in India, known as the Wireless Experimental Center (WEC), was now undertaken at Arlington Hall.

The order of battle intelligence derived from daily lists of the addressees of Japanese Army units was a useful adjunct to the text of the messages and even supplied knowledge of military operations in periods when the messages themselves were not readable. Thereafter, despite repeated changes and innovations made by the Japanese in their cryptographic systems, solution was continuous, though on occasion it was temporarily delayed. The knowledge of Japanese cryptographic practices and previous solution of the basic code book permitted the reading of periods which, from a cryptanalytic point of view, were as difficult as the systems encountered at the time of the Pearl Harbor attack, systems which had then been considered hopeless of success.

Two major technical problems which had to be solved in 1944 were the introduction by the Japanese on 1 August of a new cryptographic practice which disguised the system indicators and a radical shortening of the life of one of the keying elements used in the Administrative systems. The uncovering of the disguise in the case of each system indicator was, of course, a prerequisite to the subdivision of intercepted messages into their respective systems preparatory to any other steps toward solving or reading the messages. Though the introduction of this feature might have been a major cryptanalytic disaster, it fortunately turned out to be only a nuisance, because it was at first effected by an insecure method, and speedy solution was therefore possible. Subsequently the Japanese modified the method to the point where, had it been used initially, solution would have been almost impossible. With continuity of solution, however, aided by information from cryptographic instruction messages and captured materials, this handicap was overcome.

The problem presented by shorter intervals (five days instead of three weeks) between changes of keys, was essentially one of carrying on analysis of one of the steps of encipherment with only about a fourth of the traffic previously available, was eventually solved by a combination of methods, namely, very careful correlation of every piece of intercepted traffic, the use of tabulating machinery, which enabled a tremendously large number of operations to be made in a short time, and the use of photoelectric equipment to exploit phenomena resulting from messages with identical or nearly identical text but cryptographed with different keys.

Once the Japanese began to suffer military reverses, their cryptographic materials were frequently captured and these soon came to play

a vital role in solution. Especially important was the capture of the basic code books, or of the key books which the Japanese could not easily replace with new editions and which therefore were occasionally continued in effect for some time after their capture. The complete reconstruction of such code books and key books would have been a long and painstaking task which would have resulted in delays in production of intelligence and possibly also in some diminution of its reliability. Yet the continued capture of such materials was not an unmixed blessing, since whenever a capture was known or even suspected, the Japanese naturally changed as many of their other cryptographic materials as possible.

Thanks to the care with which information obtained from the translated messages was used by field commanders, the Japanese seem never to have suspected the possibility of cryptanalytic compromise but, as they began to realize that Allied Forces were able to anticipate their plans, they attributed our success to espionage activities. The following extracts are taken from a message, intercepted and read by the SSA, which was sent from Pinrang to Piru (RIIA Communications Officer) on 18 December 1944 (Japanese serial number 893, SSA Bulletin number J-8092-A-I):

> " . . . . there are substantial indications that the enemy has understood our important plans in the Burma and Philippine areas. Therefore, we are inclined to be somewhat doubtful about the codes now in use [and] each unit commander must multiply his alertness toward counter-espionage . . . . This is an order. Furthermore, you should exert your best efforts towards overcoming the deficiencies in the counter-espionage set-up, and towards perfecting it. If you fail to do this, troubles will arise, and you must take resolute action in facing them, without a thought for yourself."

Because of actual or suspected compromise, however, changes were made so frequently and complications so often introduced in the Ground systems that analysis became more and more difficult. By the end of the War the Ground problem reached the point where the time required for solution made the production of current translations seemingly impossible. The general intelligence value and the special cryptanalytic interest of the problem, however, warranted studies of the last unsolved period of the highest-echelon Japanese Ground Force system, for which no captured material or special cryptographic intelligence were available. These studies, successfully carried out during the final months of 1945, demonstrated that the development of cryptanalytic attacks had kept pace with the ever-increasing complexity of Japanese cryptographic procedures.

On the other hand, no compromises or suspected compromises took place in the case of the Water Transport systems, and in the latter the Japanese moved in an orderly fashion to make their periodic changes. Consequently, the cryptanalysts were less hampered by frequent or sudden changes and a

fair proportion of the messages in each key book were read currently. Had no compromises been made in the Ground systems, the same success might have been experienced. Therefore, it is a moot question whether compromised material gave an overall advantage or not.

For lack of sufficient personnel and because of the special interest of GCCS in the Air systems, the SSA did not concern itself to any considerable extent with these systems until late in 1944. Thereafter, more and more attention was devoted to the air problem and the SSA eventually made large contributions to current solution.

After some early compromises in 1944 the Japanese signals systems were read from time to time. The cryptography used was such that, with the limited volume of traffic, solution would have been extremely difficult without a compromised code book, but fortunately at different times several successive editions of the signals code books were captured, along with the key books for a number of periods. The text of these systems, which discussed call-sign frequencies, and methods of handling traffic, was of special interest primarily to our traffic analysts.

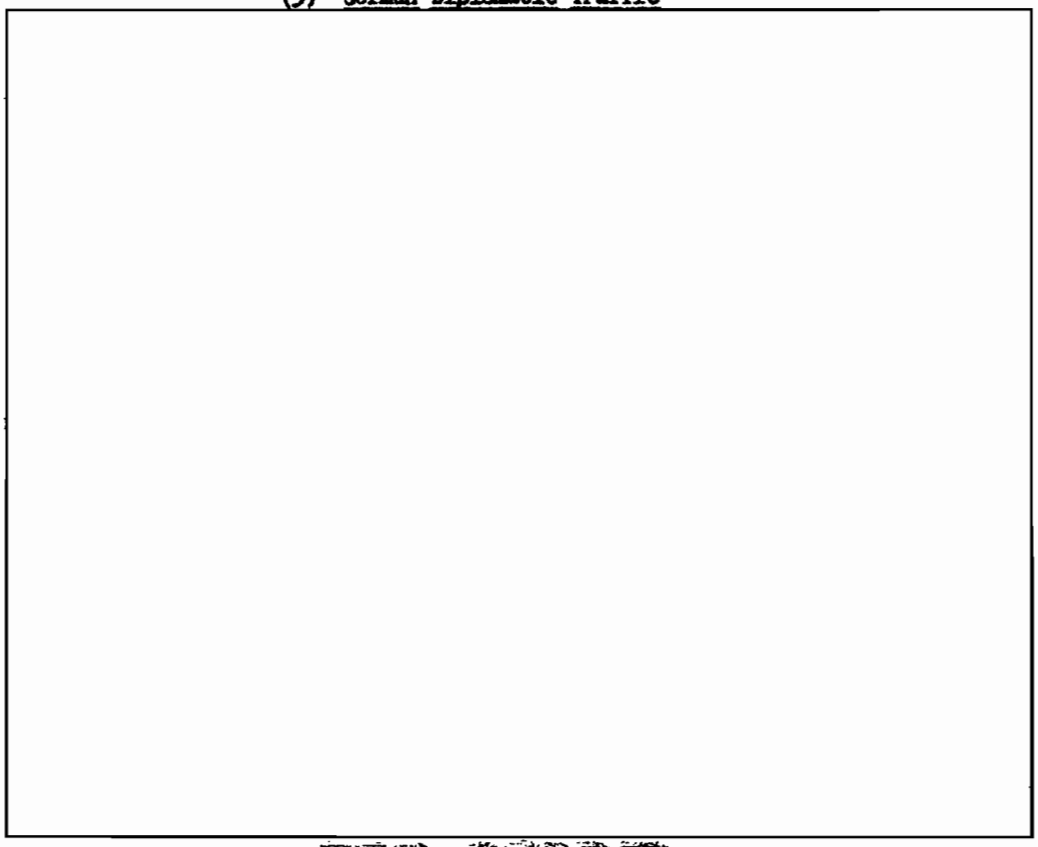
While the study of low-echelon Japanese systems was never considered a primary responsibility of the SSA, reports from field agencies were examined here and their contents served as a guide in the training of military personnel destined for field agencies. The SSA did actively participate in the solution of the low-echelon air system known as "BULBUL" but only as a support for the cryptanalytic unit in the India-Burma Theater.

The impression has already been given that had more personnel been made available and at an earlier date, solution of Japanese military communications might have been expanded and expedited. Yet it should be pointed out that had all the U. S. Army personnel working on the Japanese Army problems, not only at Arlington Hall Station but also in the Central Bureau at Brisbane, in the Hawaiian Islands, and in the India-Burma Theater, been grouped together at one center and solution activities thus been concentrated, considerable unnecessary duplication, especially in the field of translation, would have been eliminated. On the other hand it must be admitted that had such a consolidation taken place problems of administration would have been greatly increased but the advantages gained by the increase of trained workers all applying their efforts in a coordinated attack would have outweighed by far any administrative difficulties. As it was, where circumstances permitted, duplication was eliminated and, considering the great distance between the agencies concerned, cooperation and coordination effected by the interchange of mail and telegraphic communications was good.

In retrospect, it may be noted that in the signal intelligence field the consequences of lack of continuity and unpreparedness for effective operation immediately upon the outbreak of hostilities are nowhere more clearly demonstrated than in the case of the Japanese Army high-echelon

secret communications. It is a fact that during the entire period from 7 December 1941 to the summer of 1943, none of these communications was being read. Had this been otherwise, the military situation might have been quite different. To judge purely by the disastrous effect that the solutions obtained by us after the autumn of 1943 had upon Japanese operations, it is legitimate to think that the important early Japanese penetrations to the south might have met with greater obstacles and that as a result the War in the Pacific might have been terminated many months earlier. If an adequate staff of cryptanalysts had been engaged in studying Japanese Army traffic continuously from 1939, when the systems were solvable with comparative ease, complete continuity could have been maintained from the very outset of the War. After 1939 the systems became more difficult but never more difficult than they were in 1945 when, because of the possession of a background of knowledge and experience built from successful reading of earlier periods, they were solved.

(3) German Diplomatic Traffic



(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(4) German Army and Air Force Traffic

It has already been noted that a logical division of work between the British and the U. S. Governments resulted in concentration of the SSA on solution of Japanese diplomatic communications and Japanese military traffic in the Pacific theater, leaving the exploitation of German and Italian military traffic in the European theater the primary responsibility of the British. When it is understood that the latter traffic required an organization of over 10,000 people at the largest British processing center (GCCS) near London, and thousands more in the field to intercept the traffic, forward it, etc., the wisdom of this arrangement becomes obvious. In the tense days of early 1942, however, the advisability of insuring against the contingency that the British organization working on enemy communications might be put out of operation by enemy action led to the establishment of an SSA unit to serve as a back-up. Though the SSA played the minor role in the work on German Army and Air Force and Italian Army and Air Force traffic, nevertheless it made noteworthy contributions.

The German Armed Forces employed two basic types of cipher machines. One of them, a modification of a commercial machine known as the Enigma, produced cryptograms of a very high order of security, but faulty usage, Teutonic love of order, and addiction to stereotyped modes of expression made it possible for the British to solve a very large portion of all the messages transmitted, yielding intelligence of the highest value. In this work the SSA served as a cooperating and assisting echelon, contributing new ideas, techniques, and machinery. As a result of excellent coordination of basic research and development with practical operations SSA engineers invented and built an electronic solution machine far in advance of anything hitherto known for solving messages in the most complicated form of the Enigma machine as used by the Germans.

In addition to the foregoing, specially selected messages were sent from England to Arlington Hall for study and solution by SSA special machinery. The necessity for speed brought into use special communication channels and there were cases wherein the answer to a specific problem was obtained by the SSA, wired back and in the hands of the GCCS cryptanalysts within 90 or sometimes as few as 60 minutes.

The SSA also assembled and basically trained a large group of technicians who were then sent to England to function as Signal Corps units under the supervisory control of the Director of Signal Intelligence, ETO, but working in the British units with British technicians in a combined attack on the Enigma problem. Three special radio intelligence detachments were established: the 6811th intercepted Enigma traffic, the 6812th operated special solution machinery provided by the British, and the 6813th engaged in processing activities. The contribution of these units in the solution of Enigma traffic was very important in the overall picture of SSA activities.

The German Armed Forces also used a series of complex cipher machines for enciphering teleprinter communications among their highest echelons. Here again the SSA collaborated with the British in inventing and designing new machinery as well as in testing new techniques and procedures. Two machines in particular, invented, designed, and built either entirely at Arlington Hall Station, or by an outside contractor working under the direction of SSA engineers, were then shipped to England; both were successfully employed by British technicians, assisted by SSA experts, in work on these teleprinter communications. In addition to making an important contribution to the victory in Europe, the experience the SSA gained in such collaboration will, of course, be very useful to the U. S. Army in future research in this field.

Mention must also be made of our contribution in the signal intelligence operations in the Mediterranean Theater. Here again the SSA furnished key and basically-trained personnel for Signal Corps units working in collaboration with British forces on both German and Italian secret communications.

(5) [redacted] traffic

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Royalist Governments presented no great difficulty. One important result of the surrender was the receipt of a large body of captured cryptographic material going back over thirty years. Tests of the American reconstructions against the photographed Italian originals showed that the former were remarkably correct; the accuracy of the translations made from the reconstructions closely approximated 100 per cent. Additional valuable information was derived from participation in the Cipher Security Mission in Rome in 1944 and 1945. When the Italians were finally allowed by the Allied Control Commission to introduce newer systems, the SSA was well equipped to begin a new attack.

(6) Other Diplomatic Traffic

Mexican diplomatic systems were studied as early as 1938 and gradually the attack spread to cover other systems in the Spanish language, including not only those of Spain itself, but also of all other Spanish-speaking countries except only Honduras and Paraguay, which use cryptography so little that the supply of traffic is inadequate for solution. From 1942 to 1943 all of these systems were reduced to a production basis: as fast as new systems appeared, they were solved.

Portuguese and Brazilian diplomatic systems were first studied in 1941, intensively after 1942, and by the summer of 1944 most of these had become readable. The importance of Portuguese traffic is, of course, obvious: Lisbon, as one of the few neutral capitals, was a valuable center for information.

French systems (those of the Vichy Government were first studied in 1941) involved the concerted efforts of a large staff since one of the basic tenets of French cryptographers is that a multiplicity of different systems in simultaneous usage, with frequent minor changes therein, will result in great security. Since both the Vichy and the Free French Governments followed these principles, ultimately several hundred French systems were known, and a great many of them were made readable. The traffic of the Swiss Government provided cryptanalytic problems of moderate difficulty and owing to the fact that the Swiss served as representatives of belligerents in many countries, Swiss traffic was an important source of information. Work was also carried on, though on a smaller scale, in Belgian, Haitian, Luxembourg, and Rumanian traffic.

Late in 1942 work was initiated on the systems of those governments which use the Arabic and Turkish languages. After a modest beginning, the traffic of the following governments was read: Egypt, Ethiopia, Iran, Iraq, Lebanon, Saudi Arabia, Syria, Transjordania, and Turkey. Of these, by far the most important in production of valuable information and in extent of the task of solution were the Turkish systems.

Attention was first extended early in 1943 in the Far Eastern field to systems used by governments other than the Japanese. Ultimately, these included the Chungking Government of China, which formed the bulk of the effort, the Nanking Government of China, and the puppet government of

Thailand. Of interest in the latter connection is the fact that though the SSA was successful in recruiting an expert in the Thai language, the system was found upon solution to be in English. The linguistic problem presented by the Chinese systems was likewise occasionally simplified by their use of English.

Not until 1944 was it possible to begin the study of the traffic of a group of Central European governments which ultimately included the Nazi Government of Bulgaria, the Royalist Government of Yugoslavia, the puppet government of Croatia, the Czechoslovakian Government in London, the Slovakian puppet government, the Polish Government in exile, the Royalist Government of Greece, and the Nazi Government of Hungary. Solution of these systems was complicated by the difficulty of obtaining competent linguistic experts, but in the end one or two systems of each of the governments named had been made readable.

(7) Weather Traffic

In peacetime information concerning the weather, and predictions of future weather, are very important for most people, and large organizations exist in many countries for the collection and elaboration of weather data. Such data are usually transmitted in a universal code called the International Meteorological Code, known to all countries. During wartime, in military operations, especially those involving aircraft the importance of meteorological observations and data to forecast weather conditions over limited or extensive areas in the combat zone need hardly be emphasized. It is for this reason that such information must be sent in cryptographic form, usually by enciphering the basic data as encoded in the International Meteorological Code.

Beginning in June 1942 and continuing for about two years a unit was maintained to study the various cryptographic systems used for this purpose by enemy and associated powers. These efforts were handicapped by several factors: difficulty of obtaining adequate coverage in time to make the information useful, lack of knowledge of climatological conditions, particularly in the Far East, and technical difficulties. But the efforts to solve the systems used by the French, Italians, and Germans in Europe, and by the Japanese in the Far East ultimately proved successful. By this time, however, it became increasingly clear that, in order to avoid unnecessary duplication of effort with this problem in which the Navy was also, of course, interested, it would be more efficient to confine efforts of the SSA to the training of field teams, to research and development of techniques, and to coordination of all units in the theaters of operation. By an agreement with the Navy, reached as the result of a Joint Conference of Army and Navy officers held on 7 April 1944, both services were to continue interception, research and development in the field of weather traffic, while the Navy undertook responsibility for the exploitation of the main Japanese weather system. A full exchange of technical information was to be made and the Navy would disseminate weather intelligence to Army users. Thereafter, day-to-day solution of Japanese weather traffic was

abandoned by the SSA.

(8) Commercial Code Traffic

Exploitation of the information to be obtained from decoding traffic sent by business houses and private individuals in public commercial codes was carried on more or less continuously after early 1943. This activity was at first confined largely to codes in the chief languages of Europe but was ultimately extended to include also a group of Japanese commercial codes which provided a rich mine of militarily useful information concerning conditions in the Far East.

(9) Special Problems

In addition to the traffic already described, the SSA had to face a number of other special problems requiring other techniques. These included the transcription of shorthand documents; the solution of open codes, a type of cryptography in which a secret text is hidden within an ostensibly harmless message; the transcription and translation of "scrambled speech," that is, telephonic and radiotelephonic conversations in enciphered and unenciphered form in foreign languages; and the solution of secret ink messages. The last named type involved much work for the Office of Censorship as well as for MID. In this field the SSA technicians accomplished feats not duplicated elsewhere: the recovery of printing on documents which had been printed by use of inks soluble in water. In the case of two documents very valuable code materials were recovered for the Navy; one involved a German, the other a Japanese code book.

E. Some General Remarks

The remarkable success which the cryptanalytic units obtained must not be allowed to create the impression that any of the tasks was accomplished without skill, training, patience, vigilance, and mental labor of the most exhausting kind. A description of the essential features of a solved cryptographic system may often seem simple and it may be imagined therefore that solution was easy, but this is rarely the case. Frequently, a simple cryptographic trick may be as difficult to detect as one of the more complex varieties; in cryptanalysis the effect of some minor complicating factor, inserted solely to prevent solution, may prove to be a serious stumbling block though occasionally it may also prove to serve in the end as the entering wedge leading to solution.

The time and effort needed for solution, of course, vary with the system. A simple substitution cipher may require only a few minutes' work by a single analyst; other systems may be so difficult that the entire efforts of a number of persons working for many months are needed. Of the two basic types of cryptography, codes and ciphers, reconstruction of the former is, as has already been noted, a slow, laborious process, each

code group having to be identified singly, and the larger the code, the longer the time needed; solution of a difficult cipher may take equally long but success is instantaneous rather than gradual—at one moment the cipher is unsolved, the next it is solved. The reconstruction of a cipher machine is, of course a very long process, but when this is finished, the keys used in each day's traffic may still have to be solved as they appear. For this reason, even when the machine has been reconstructed, reading of current traffic may be delayed until enough traffic all in the same specific key has been received to permit solution.

Systems differ so greatly that a counting of solved systems is no adequate indication either of the volume of work accomplished, or of the brilliance of the achievement of the cryptanalysts. During the War a group never numbering more than twenty, and for a long time many fewer, succeeded in making readable approximately twenty-five systems. In the same period a group of about eighty persons were needed for the solution of a single system. For this reason the efficiency of the two groups cannot be evaluated in terms of the number of systems solved.

A somewhat better indication of cryptanalytic accomplishment is that furnished by the number of governments of which the traffic was made readable by cryptanalysis. At the beginning of the War the cryptanalytic attack was centered, as we have seen, only on four governments (Japan, Germany, Italy, and Mexico), though a start had recently been made on the traffic of a few other governments. By August 1945, however, the traffic of more than sixty governments had been studied and translations were currently being prepared in large volume. The number of these translations is really the best gauge of the cryptanalytic achievements of the SSA, since they are the final products of the cryptanalysts, assisted by the combined efforts of intercept operators, clerks, translators, editors, typists, and proofreaders. A figure in the Appendix (No. 10) shows the rise in daily volume of translations throughout the War. It should be pointed out that every message counted in this tabulation was sent in cryptographic form: no plain-text messages were included. Factors causing fluctuation of volume were complex: it is not always possible to explain declines, but on occasion the introduction of new cryptographic techniques had the effect of slowing up production temporarily until solution was achieved.

After cryptanalysis the messages in almost every instance still had to be translated—a small percentage of the messages are transmitted by their originators in English—and after the translations were prepared in draft form, they had to be checked for diction, accuracy, and format, and then typed for reproduction by the "Ditto" process. "Master copies" of the translations were then once more proofread for accuracy of typing and the required number of copies prepared. Following this, they were forwarded at frequent intervals during the 24 hours to MIS. In certain cases, where urgency required it, forwarding was either by special courier or by electrical means, over special cryptographic circuits.

Even then, the task of the SSA was not finished, for it was necessary that the daily "SSA Bulletin" of translations be read carefully by personnel whose duty it was to compile therefrom voluminous information which would, in turn, be useful to the cryptanalysts working in other problems. Thus the fruits of the labors of one working unit could be at the disposal of any others that might need it. In this connection it may be stated that the free exchange of information and results among the traffic analysis units, the cryptanalytic units, the translation and "bulletin" units, the communications-security units, and so on, is absolutely vital to success in the whole cryptologic field.

F. The Pearl Harbor Investigation

As this report is being prepared, the daily press is giving much attention to the testimony disclosed at a Joint Congressional Investigation into the causes of the Pearl Harbor disaster. While the investigation is not yet complete, all testimony thus far disclosed has demonstrated the incontrovertible fact that in the period prior to the attack the SIS was performing the function for which it was intended: Japanese messages were being translated and forwarded to MIS in considerable daily volume. In this connection the testimony of Major General Sherman Miles, who in December 1941 was Assistant Chief of Staff, G-2, as reported in the Washington Evening Star on 3 December 1945 (p. A-4) is of the greatest interest:

> "Mr. Gesell [counsel for the committee] informed the committee he will be prepared later to offer a detailed record of the handling of important Japanese messages intercepted during the week before December 7, 1941, but not decoded and translated until a week or more after the attack.
>
> "Mr. Gesell said he is gathering data to show the monitor stations that picked up each message, when it was transmitted to Washington, whether by airmail or radio, and when it was received for decoding.
>
> "In discussing the delay in decoding these messages today, General Miles told the committee:
>
> " 'The astonishing thing, gentlemen, is not that these messages were delayed, but that they were able to do it at all. It was a marvelous piece of work.' "

Attention has already been drawn (see page 19) to possible causes for the interval which in some cases elapsed between the date of interception and the date of translation. It should be pointed out here that it is impossible to tell from the raw traffic which message contains important information and which does not. Only after all the messages have been reduced to plain text can persons familiar with the language pick out the valuable items and give them priority in translation.

In making public earlier reports of investigations of the background of the Pearl Harbor disaster, the Government for security reasons withheld certain passages. As had now been made clear by the current Congressional investigation, these passages contained references to the success of the SIS in solving the Japanese most secret diplomatic system. The reasons for concealing this fact were based upon two considerations. In the first place, it was imperative that every effort be made to prevent the Japanese from learning that their most secret diplomatic system had been solved, for if they did learn that fact, they would most certainly either abandon the system entirely, in which case the work of the best cryptanalysts for more than two years would be nullified, or they would change as many elements in the enciphering process as conditions of distribution would permit. In either case, the loss to current military intelligence would have been tremendous, as General Marshall eloquently pointed out in his letter to Governor Dewey already cited. With the cessation of hostilities, of course, this consideration loses its force, but there was another consideration, in the long run much more vital to the defense of the United States. Any success in solving a cryptographic system, if disclosed to the general public, has the immediate effect of stimulating other governments whose messages may now or at a later time be under study to endeavor to improve their systems in such a way as to render them impregnable. This is, of course, the aim of all cryptographic compilation bureaus at all times: knowledge that a given type of cryptography has been solved by any government will at once greatly accelerate the process of research and development.

The publication in 1931 of Herbert O. Yardley's indiscreet book, The American Black Chamber, had, indeed, precisely this effect: many governments, including some which were not even mentioned in the book, at once began to prepare new types of cryptographic systems which would at least not be open to the specific kinds of attack which Yardley had shown to be successful. The cryptographic techniques which had been regarded as adequate in World War I were infantile when compared with those encountered in World War II. Had Yardley's book never been published, such a development in the cryptographic art might never have taken place.

Now that the solution of the Japanese cipher machine has been disclosed to the world, all governments have been given notice that even a system of such high security as this is not invulnerable to attack. That several governments were aware of the system is a good presumption: at least two (the British and German) are known to have attempted solution without success and their cryptanalysts may well have regarded a machine cipher of this type as indecipherable. Not only these two governments but all others now know the contrary, and the race for a really indecipherable system will henceforth become much keener. It is not beyond the range of possibility that other governments will achieve success and that in a future war the enemy may have provided himself with an absolutely secure system. The consequences of such a state of affairs to the gathering of military intelligence are, in the light of the recent development of the atomic bomb and its effect upon military techniques, incalculable.

III. THE PRESERVATION OF SECURITY

The preceding chapter has shown both the potentialities for intelligence purposes inherent in the study of enemy communications and the extent to which, through the successful activities of the SSA, the War Department and the Army were able to exploit these potentialities in the prosecution of World War II. We now come to the really more important obverse side of the picture: the protection of our own communications against enemy signal intelligence services, for it was to be presumed from the experience of World War I that other governments would also maintain such services to subject our communications to careful scrutiny, a presumption which was, indeed, fully confirmed throughout World War II. Enemy messages solved by us gave clear-cut evidence that the three major Axis powers did endeavor to derive intelligence from our communications; and special operations since the cessation of hostilities have added much to our stock of information concerning enemy signal intelligence activities, successes, and failures.

In considering protection against enemy operations of this type, the goal sought was the development of techniques and machinery that would effectively prevent all possibility of deriving useful intelligence from any of our communications, no matter how voluminous they may be and without regard to the conditions under which they must be prepared or handled. But the experience of many years of development in the cryptographic art has shown that the attainment of this goal still lies in the future; even relative security may be regarded as high achievement when one considers the many factors and difficulties that enter into the problem. In a brief report such as this must be, it is possible only to indicate in very general terms what these limiting factors and difficulties are and how they were met.

The use of radio in military communications had its real beginnings in World War I, and since then so important have been the successive developments in the science that the extent to which the successful conduct of large-scale warfare is now dependent upon such communications needs no emphasis. Code methods, although they were very slow in operation, then predominated in military cryptography, and cipher methods, even though a bit more rapid, were generally too insecure, or, if secure, too cumbersome or complex for practical purposes, so that the latter methods played only a minor role. So far as concerned the SIS in its early days, this growth in the employment of radio meant first that, unless more speedy means and methods for protecting the voluminous traffic against enemy solution than were known or in use up to that time were developed, cryptography would constitute a most serious impediment to effective signal communication. Secondly, it meant that, unless more secure means and methods were devised for this purpose, the traffic would probably be more or less readily solved by the enemy because of the sheer bulk of messages in the same code or cipher system. It was soon recognized that both of these needs, greater rapidity

and higher security, could only be satisfied by the invention and development of special machines for the purpose, and even before 1930 much attention had been devoted to these problems. Progress was, however, very slow because of the paucity of available funds and also because greater emphasis was placed upon the development of radio communication apparatus than upon that of means to protect the communications transmitted thereby. But within a few years after the SIS was established such important progress had been made in the latter field that it brought about not only the development of cryptographic means which were both speedy and secure but also caused what practically amounted to a revolution in cryptographic theory and practice: codes came to be replaced almost entirely by cipher methods, resulting in profound changes in security techniques and practices.

Obviously, had it been possible to design a single machine which could serve all the many different requirements of fixed and mobile cryptographic communications, steps toward that end would have been undertaken, for even in 1930 such a goal was clearly recognized. But it was not possible then and it is still impossible today, for a variety of reasons, only the most salient of which can be briefly discussed herein.

In military signal communications provision has to be made for many different types of users but in the main these may be roughly classified under the heading of three categories:

a. Administrative systems used for communications between high echelons such as the War Department, theater headquarters, and the like;

b. Field systems used by large, intermediate, and small ground or air units in actual military operations;

c. Special systems for specific purposes other than the foregoing, such as those required for military attachés, military observers and missions, etc.

The permanence of the fixed installations transmitting traffic of the first type in general impose fewer restrictions upon the ingenuity of the designers of cipher machines; size and weight are of relatively little importance and the best cryptographic techniques can be utilized with few limitations. On the other hand, in preparing for field use, all sorts of limiting factors enter the picture, such as portability, compactness, sufficient ruggedness of equipment to stand up under the conditions of warfare and tropical climates, difficulties of distribution, dangers of capture, adaptability of the system for use by relatively untrained personnel, and the like. Such factors usually prevent the use of the most secure techniques known and necessitate the adoption of systems which, while lacking in one or more of the desired features essential to complete security, nevertheless are suitable for the practical conditions encountered in the field, since tactical messages, in contrast to administrative, are usually brief and require a shorter period of security.

Furthermore, the systems have to be adapted for use with a number of different media of signal communication. These include not only such media as are involved in the so-called "record communications," where written messages are transmitted in the Morse alphabet (dots and dashes) by telegraph, cable, and radio, but also media utilising "voice communications" and "picture communications."

In World War II not only was it necessary to invent and develop such machines and systems for protecting transmissions by all these media but they had to be produced in the quantities required, stored until ready for distribution, and then distributed all over the world to users with proper observance of security precautions. Each document or device had to be accounted for with absolute accuracy. Replacements for all systems had to be on hand at all times because of the continual danger of physical or cryptanalytic compromise. Moreover, cryptographic personnel had to be adequately trained in the operation and maintenance of all authorized systems. To keep a permanent check on the adequacy of current cryptographic systems and the methods by which they were being used, and to determine future requirements, message traffic had constantly to be monitored or otherwise procured for analysis. Violations of security had to be detected and corrected in order that they might be reduced to a minimum, since one of the most profitable aids to cryptanalysis is the exploitation of errors made by cryptographic personnel.

Long before the Pearl Harbor attack the foundations essential to carry out these functions had been soundly laid to permit the tremendous expansion necessitated by the War. To fulfill these functions only 26 officers and civilians were at the disposal of the SIS on 7 December 1941. Only a half dozen or so basically different systems were then in effect, with fewer than 100 separate keys. Changes in cryptographic keying materials were made at relatively infrequent intervals, since with the small volume of traffic being transmitted in peacetime it was possible to use these materials for longer periods.

In July 1945 the organization at the SSA for cryptographic compilation, distribution, accounting, and security studies comprised more than a thousand officers, enlisted men and women, and civilians. Cipher machines of several different types had been invented, manufactured in large quantities and distributed to thousands of holders (for a graphic representation of this expansion in terms of growth of number of systems in current use and of number of holders, see figures 11 and 12, respectively); a large printing plant had been built; vaults adequate to store vast quantities of documents and machines had been constructed; couriers carried the frequently changed cryptographic materials to the four corners of the world; maintenance and repair shops for keeping the cipher machines in good serviceable condition had been established; training literature and courses of study in maintenance had been elaborated; schools for training

maintenance, cryptographic, and security technicians had been established; and everything essential to safeguarding the communications of the vast military networks had been provided. The result was that the U. S. Army was better equipped for cryptographic communication than was any other Army in the world. It had the most rapid, most secure, and most efficient cryptographic machines and its personnel were the best trained in security practices. How far it surpassed the armies of its enemies in these respects will be told later; the achievements of the SSA are all the more striking when consideration is given in this connection to the fact that cryptographic communications and high standards of security of communication are hardly necessary or found in civil pursuits, so that competent personnel are unavailable to begin with and must be trained for the purpose.

The security equipments which deserve principal attention, are, as designated by their short titles, as follows:

a. Apparatus for record communications (cipher machines)
   (1) SIGABA
   (2) SIGCUM
   (3) SIGTOT
   (4) SIGNIN
   (5) "CCM"
   (6) Converter M-209

b. Apparatus for voice communications (ciphony machines)
   (1) SIGSALY
   (2) SIGJIP
   (3) SIGRIT

c. Apparatus for picture communications (cifax machines)
   SIGMEW

Taking up apparatus of the first category, the SIGABA, or Converter M-134-C, illustrated in the Appendix (No. 13), was the result of a long period of research and development which had been begun by the SIS as early as 1925. It was preceded by a less efficient model known as Converter M-134 which, because of lack of funds, had been put into production on only a limited basis prior to the War. The earlier model employed a keyboard, a feature that permitted rapid operation, and was based upon excellent cryptographic principles, using electrical connection-changers or "rotors" which, by rotation on a shaft, constantly change the connections between the keyboard and the printing unit so as to vary the relationship between the plain-text letters and their cipher equivalents. The rotation or stepping of the rotors was controlled by an external element (in this case, a keying tape), not an intrinsic part of the machine itself and provided a simple means for irregular or aperiodic stepping of the rotors, a feature that was new, extremely important, and arose from extensive cryptanalytic studies of an earlier, insecure machine, which, though of generally similar design, produced periodic repetitions in the key sequence.

Much work had been done on the development of the M-134 and the stage of negotiating contracts with manufacturers for the production of the machines in volume had been reached when, in 1935, SIS personnel conceived the idea of substituting for the external keying tape an internal, electrically simple but cryptographically complex, mechanism which would provide the long irregular sequence used for keying. In spite of the fact that these technicians thought the new control mechanism far superior to that used in the M-134, negotiations for production of the M-134 in volume continued, since the administrative heads of the SIS feared that if a further delay in production, caused by the need for additional experimentation, should occur, the Army might face an emergency without machines of any type on hand. Accordingly, the new principle was laid aside for the moment by the Army. But a few months later, when the Navy, dissatisfied with its current machine, was searching for better principles to incorporate in a new model, the Army communicated its ideas regarding the internal control mechanism to the Navy, with the result that the Navy adopted this feature and developed a highly satisfactory model. Additional collaboration between both Army and Navy experts led to further development of the machine and ultimately both services joined in letting contracts with the Teletype Corporation for a large number of machines, which became known in the Navy as the Mark II ECM (CSP 888) and in the Army as Converter M-134-C, or SIGABA. The superiority of this joint machine to its Army predecessor, the M-134, lies chiefly in the fact that, though equally secure, it is much more rugged for practical purposes; since no tape is required, it also involves fewer difficulties in distribution.

Meanwhile, procurement of the M-134 had proceeded by September 1939 to the point where 12 converters were on hand and 10 more on order. At this point certain mechanical improvements were made in the M-134 and these were incorporated into the 10 converters then on order and into 12 others ordered at that time: these 22 converters were therefore given a slightly different number (M-134-A). In all, there were ultimately manufactured 75 Converters M-134 and M-134-A, many of which were in service long before December 1941. They carried the great bulk of the secret and confidential high-command traffic of the War Department for some time after 7 December 1941, for although by that date the Navy had let contracts, in which the Army was to share, for a total of 586 converters M-134-C, delivery was so slow that by 23 December 1941 the Army had been able to distribute only 45 of the machines. By the summer of 1942, however, enough SIGABA converters were on hand to replace all the Converters M-134 and M-134-A.

The SIGABA continued during the War to be the most secure electromechanical cryptographic system in use by any government. Constant attempts by cryptanalysts in the SSA to analyze SIGABA traffic have resulted uniformly in failure. Indeed, evidence which has come to light since the cessation of hostilities has revealed that though the Germans knew of the machine (they called it "the big machine"), they had had absolutely no success in solving SIGABA traffic; nor had the Japanese. The equipment weighs 137 pounds, is therefore semiportable and can be used in mobile as

well as fixed message centers. Although keyboard operation by trained personnel permits an operating speed of 45 to 50 words a minute, this comparatively quite excellent speed is still not sufficient for certain operations. The inadequacy led to a joint Army and Navy project covering the research, development, and construction of the so-called "auto-aba," a machine which permits high-speed operation of the SIGABA by means of perforated tapes: an outgoing message is first prepared in the form of perforated tape; the latter is passed through the "auto-aba" where the message is enciphered and emerges again in perforated-tape form as a cryptogram; this tape can then be fed through any teletype transmitter and sent as a teletype transmission. At the receiving end, the cipher tape is fed through the "auto-aba," the resulting decipherment is in the form of a perforated tape and the latter can then be caused to print the deciphered message on a teletype printer.

The "auto-aba," however, was not perfected until almost the close of hostilities. In the meantime the tremendous volume of messages exchanged among the many large administrative centers of the Army by teletype facilities indicated that there was urgent need for teletype cryptographic apparatus. The need was met by the development of two types of machines to be directly associated with the teletype apparatus itself. The first of these was the SIXCUM, a machine invented by SSA personnel and developed under their direction by the Teletype Corporation (see the illustration in the Appendix, No. 14). Attempts to devise machines for protecting teletype communications go back to World War I, when the American Telephone and Telegraph Company, working in close conjunction with the Research and Development Division, Office of the Chief Signal Officer, had developed a system and apparatus for cipher printing telegraphy. But the apparatus was not cryptographically secure and the coming of peace had caused the dropping of the project.

With the imminence of World War II, research and development of this project was resumed by the SIS. An important invention in 1939 culminated in the introduction in 1943 of a new converter, the M-228 (SIGCUM), which permits the simultaneous automatic encipherment, transmission, reception, decipherment and printing of teletype communications. By the summer of 1943 the new converter was being used extensively between the United States and overseas theaters of operation. The M-228 had been designed expressly for use with wire transmission, not for radio, but owing to the pressure of circumstances, it was employed on radio for a short time for secret and confidential communications; soon, however, as a result of security studies which cast some doubt on the security of the machine, its use was limited for radio transmission to confidential messages, although it continued in use for secret messages when transmitted entirely over wire lines. Subsequently, an adaptation of SIXCUM known as SIGHAD was developed which produces a key of sufficient length to encipher continuously for a period of twelve hours without repeating any part of the key. This was secure enough so that even secret messages could be transmitted by radio-teletype.

One of the important features of the SIGCUM and SIGHAD machines is that they permit what is called "on-line operation". That is, the two ends of the circuit are so arranged that by typing the plain text on a keyboard at the sending end, the message is enciphered, transmitted, received, deciphered, and printed at the receiving end, all in a single step. Naturally, this type of operation greatly speeds up teletype communications and is highly desirable. But because the SIGCUM was not secure enough to handle Top Secret messages, another attempt at the solution of the problem of providing a high-security system for combining encipherment with transmission was found in the "one-time tape" system known as SIGTOT (illustrated in the Appendix, No. 14). The basic principle underlying all "one-time" systems is the use of a completely-randomized key never repeating within messages and never used a second time. This necessitates preparation of two copies of the key, one for use at the sending end, the other for use at the receiving end of the channel. The SIGTOT is an application of this principle to transmission by teletype and involves the preparation of two tapes bearing identical keys. By running the tape through the SIGTOT machine the plain-text letters are combined with the teletype signals in such a way as to transmit automatically an enciphered text which in turn is deciphered also automatically by the receiving teletype machine through which the second tape is being run. In order to insure that the two copies of the tape contain a key sequence which is completely randomized, special electronic machinery was devised by SSA engineers for the purpose. The limitations of such a system are those inherent in all "one-time" systems: difficulties of production and distribution of tapes, and the fact that usually only two correspondents can communicate by means of such a system. Where a large center must communicate with many subordinate or coordinate headquarters, a "one-time" system cannot be used for multiple-address messages unless each of these headquarters has on hand a copy of the keying tape. By multiplying the number of copies of the tape the danger to security from physical compromise is greatly increased, and for this reason arrangements for the use of "one-time" tapes with multiple-address messages has been strictly limited. This was the most serious inadequacy of the SIGTOT system. It did, however, possess that great advantage inherent in all true "one-time" systems, namely, absolute security from cryptanalytic compromise, and assurance that when key material is captured, only the specific keys captured are compromised, so that no messages other than those in the captured keys can be read by the enemy.

While discussing the subject of "one-time" systems, mention must be made that the principle was adopted for use in manual systems by the preparation of key material printed in pad form. Late in 1943 literal "one-time" pads were adopted on a limited scale for use by special War Department agents, later extended to military attachés. Since no two pairs of these pads are identical, a high degree of security is achieved.

The success attained in the use of the SIGCUM led to research and development for its improvement. This culminated in the production of

Converter M-294 (SIGHIN) during the latter part of the War. SIGHIN, illustrated in the Appendix (No. 15), is especially designed for field use of teletype. The machine is smaller and more rugged than SIGCUM, weighing approximately 100 pounds, while SIGCUM with its associated equipment weighs over 700 pounds. The cryptographic principle on which SIGHIN is based, invented by SIS personnel, is secure enough so that it can be used with all classifications of traffic on local operation, on-line or off-line on wire circuits, but only off-line in the case of radio. The security of SIGHIN was estimated in advance of tests to be approximately that of the SIGABA, in other words very high, but it is possible to read two SIGHIN messages which happen to have been enciphered by the same key. The probability of such an occurrence, however, is very slim, and should two messages be read by the enemy, the only compromise would be in the text of these two messages: no information could be derived by the enemy to compromise the entire system. The system was placed on an operational basis in 1945 and before complete reports concerning the effectiveness of the system were received, the Fifth Air Force requested a supply of SIGHIN equipment to be put into immediate operation.

Relations with the British were, of course, carried on in the field of security as in the field of intelligence but to a much more limited extent. Very early in the history of this liaison the decision had been reached jointly by the Army and the Navy to refrain from divulging to the British all information concerning the Converter M-134-C, but the problem of a system for use in combined operations with the British had to be faced. The British were willing to divulge information concerning their machine called the "TYPEX" and to supply it in very limited quantities and by December 1942 that machine was being used for this purpose to a very small extent. But later the Army and Navy jointly produced the system known as "CCM" (CCM Mark I), an adapter designed to permit messages sent with the SIGABA by U. S. forces to be deciphered by the British by means of an adapter which they designed for their TYPEX machine. By this arrangement satisfactory cryptographic means were provided for various classes of Combined Communications, and the principles of the SIGABA remained inviolate.

The need for a cryptographic system suitable for tactical use by low echelons was supplied ultimately by the adoption as standard Signal Corps equipment of a device known as Converter M-209, a small mechanical, printing machine (see illustration in the Appendix, No. 16) which superseded the M-94 in use at the beginning of the War. To satisfy the military needs the device had to be portable, rugged enough to withstand the rough handling encountered in modern warfare, and operated easily enough by relatively untrained personnel. The M-209 was not, however, a product of development by the SIS or SSA but had been invented and developed by a Swedish inventor. The SSA contributed certain improvements and models were being service tested in 1941. Large scale production began late in 1941, ultimately resulting in the manufacture of over 100,000 machines. Distribution was begun in 1942 at the time of the North African invasion. Converter M-209 weighs only 7-1/4 pounds when packed in its canvas carrying case and is hand operated, that is, it is not provided with a keyboard.

The imperfections of Converter M-209 are that it is slow, operating at approximately 12 words per minute, and that the security afforded is not as high as desired. This element of insecurity is largely occasioned by improper or incomplete training in its usage. While adequate training can be given in a few hours, experience in the field has shown that as the result of casualties, completely untrained personnel, such as truck drivers and cooks, may be forced to do the work. A security study of ETO traffic in the spring of 1944 led to the recovery of keys for a number of days and decipherment of all traffic for those days by SSA cryptanalysts. German intelligence reports have been studied to determine the extent of the enemy's knowledge of the M-209, and it was found that German cryptanalysts, using a compromised set of keys captured in the Sicilian campaign, had worked out methods of analysis which were based on the availability of messages in the same key. The greatest extent of enemy success in solution, however, was reconstruction of only five or six keys a month out of more than 5,000 in effect during the months that this device was used.

So much for security equipment for record communications: we now come to similar equipment for voice communications. The need for an even more rapid means of secret communication and one which would permit conferring by telephone and radiotelephone—in other words a ciphony (enciphered telephony) device—had long been realized by SIS personnel. Commercial speech inverters, in use in this country and employed to a considerable extent over wire lines by the British in England at the beginning of the War, were considered far too insecure for U. S. Army requirements. Consequently, attention was given to the development of equipment to provide for these needs.

Other Signal Corps agencies working in conjunction with the Bell Telephone Laboratories had practically completed development of the apparatus now known as AN/GSQ-1 (SIGJIP) when responsibility for speech apparatus development was assigned to the SSA in July 1943. Tests of the apparatus as then developed revealed that it did not meet Army requirements. Despite its disadvantages, the need for some sort of portable, simple speech equipment necessitated the use of SIGJIP, and by 1 July 1944 several units of SIGJIP equipment had been sent to the European, Mediterranean, and Southwest Pacific Theaters.

Work on the problem of developing a really secure speech system continued, however, being done in the main by the Bell Telephone Laboratories with the cooperation of the SSA, which was responsible only for the security of the system. Finally, a fixed-plant speech scrambler (RC 220-T1, known as SIGSALY) was placed in operation on 1 July 1943 between Washington and London. This equipment is far too complex to describe here (see the illustration in the Appendix, No. 17, which shows approximately one-half of one terminal. It can only be indicated that by using "one-time" keying records or a key-generating device, SIGSALY communications achieved great security, and that from July 1943 to the end of hostilities 12 terminals were in operation, so that highly secure voice communications were provided between Washington and Army headquarters

at the following points: London, Algiers, Brisbane, Manila, Honolulu, Frankfurt, Paris, Guam, Oakland, Berlin and Tokyo. Intercommunication was possible between all the terminals located in the Pacific area (including Oakland), and likewise between all terminals in the European Theater. In addition, one terminal was constructed on a seaborne barge for temporary use in the Pacific at such periods as land terminals were not yet available owing to the moving of headquarters. When Headquarters, Southwest Pacific Area, were moved from Brisbane to Manila, the terminal on the barge was towed to Manila and provided facilities available for use there long before it was possible to disassemble the land terminal at Brisbane, ship it to Manila, and then reassemble it for operation at the new location. The complexity of the SIGSALY equipment—the approximate cost of a terminal, including installation, amounted to $400,000—was such that to install, maintain, and operate a terminal specially trained personnel were needed. For this reason, the 805th Signal Service Company was activated by the Army Communications Service and a detachment of ten officers and six enlisted men, trained for three months in the Bell Telephone Laboratories, was sent with each terminal.

The great weight of the SIGSALY equipment for a single terminal (about 90 tons), as well as its large space and power requirements, effectively prevented its use in the field, where the advantages to be gained by having highly secure voice communications were most apparent. The successful development and important usage made of the SIGSALY equipment therefore led to the design and development, by the SSA itself, of a much smaller and lighter version designated as AN/GSQ-2, the SIGRIT equipment. So much reduction in size and weight was effected by intensive work and excellent engineering that an equipment that could be housed in a 2-1/2-ton trailer and therefore suitable for field use was produced. The remarkable feature of this development is that with the great reduction in size and weight there has been no serious impairment in security: SIGRIT is, for all practical purposes, as secure as SIGSALY. It is felt that SIGRIT will exercise a profound effect upon future developments in the realm of secure communications in the combat zone.

Lastly, we come to the question of security equipment for "picture communications." Development of facilities for the facsimile transmission by wire and radio of photographs, maps, diagrams, and the like, makes possible the rapid forwarding of information of great value in military operations. The desirability of enciphering such transmissions had been recognized as long ago as 1924 but pressure of other projects had prevented development of a solution to the problem. Early in 1942, however, the Third Army became interested in the use of telephoto for the transmission of situation maps and other graphic material; the AAF was also interested in transmitting weather maps securely. As a first step in the solution of this problem the SSA was instrumental in bringing about a survey by the National Defense Research Council of the previous efforts which had been made to develop cifax (enciphered facsimile transmission), and in the summer of 1943 all responsibility for cifax development was transferred to the SSA. New inventions and improvements, by SSA engineers, upon an older invention, also by SSA personnel, led to the development of high-security apparatus designated as AN/GXA-2 (SIGMEN). By its means it is possible to transmit, with high security, an excellent

facsimile of a diagram 7" x 9" in 30 minutes. Not until after V-J Day, however, was the first operational system installed on the circuit between Manila and Washington. Here again it is thought that this contribution by the SSA in the field of rapid and secure facsimile equipment will exercise an important influence upon the future of military communications, for although the present equipment is not mobile and therefore cannot be used in the combat zone in its present form, there is no doubt that it, too, as in the case of SIGSALY and SIGRIT, can be "miniaturized," so that mobile cifax equipment of high security will become available.

As the War progressed and one by one the more pressing problems were solved, it was possible to assess the achievements of the SSA thus far in the field of security. As a result, the Cryptographic Plan (SIGFRA) was promulgated in May 1945. It is a statement of the Basic Military Requirements and the extent to which equipment in current use or in the research and development stage satisfy these requirements. The thirteen Basic Military Requirements may be summarized as follows:

I. A high-security administrative system designed to encrypt the transmission as a whole.

II. A cipher machine for use between highest administrative headquarters down to and including headquarters of a field army for all classifications of traffic.

III. A cipher machine for use by field units down to and including division headquarters for all classifications of traffic.

IV. A small cipher machine for use by field units within a division for all classifications of traffic.

V. A small hand-powered cipher machine for use by field units for all classifications of traffic.

VI. An electrical machine functioning on the "one-time" principle for use by headquarters down to and including army headquarters for communications requiring absolute security.

VII. A "pencil and paper" system of highest security for special missions.

VIII. A "pencil and paper" system of high and medium security for emergency use.

IX. Cifax equipment of highest security for fixed-plant installations.

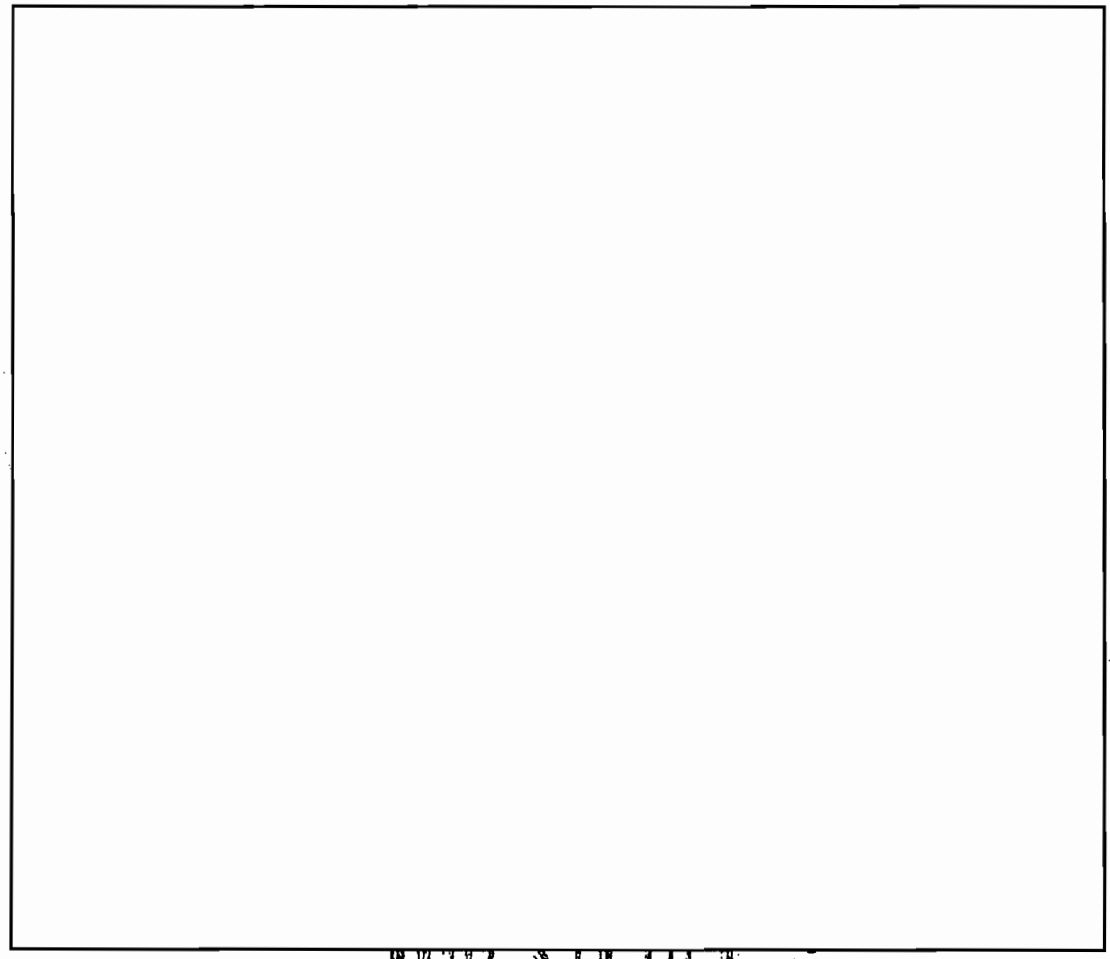
X. Cifax equipment of high and medium security for mobile field units.

XI. Ciphony equipment of highest security for use in fixed installations.

XII. Ciphony equipment of use in the field with standard Signal Corps equipment.

XIII. Ciphony equipment of medium security for use with standard Signal Corps equipment but more portable than Requirement XII.

Equipment currently in use has been deemed adequate for fulfillment of Requirements VI, VII, VIII, and XI. Equipment currently in use is deemed not wholly adequate for the fulfillment of Requirements II, III, IV, and V. Equipment now planned for interim use will, it is believed, fulfill Requirements II, III, IV, IX, XII, and XIII, and equipment planned for ultimate use will satisfy Requirements III, IV, XII, and XIII. This leaves only Requirements I and X, for which no equipment is in use or at present under development; the satisfactory solution of these two problems lies wholly in the future.



APPENDIX

1. A typical SSA unit at work.
2. Historical Outline of Code and Cipher Work, U. S. Army, 1861-1945.
3. A message from originator to MIS.
4. Letter from General George C. Marshall to Governor Thomas E. Dewey, dated 25 September 1944, reproduced from The New York Times of 8 December 1945 (page 5).
5. A Japanese message from Berlin to Tokyo describing German western fortifications.
6. A Japanese message from Berlin to Tokyo describing the German output of munitions.
7. A Japanese message from Hanoi to Tokyo showing that the Japanese were interested in uranium.
8. A Japanese message from Moscow to Tokyo showing activity of the Japanese Ambassador at the time of the Potsdam Conference.
9. A Japanese message in an unknown circuit forecasting the arrival of a convoy at Wewak.
10. Bulletin Production: Average Daily Volume of Translations of all types.
11. Number of Cryptographic Systems in effect 7 December 1941 to October 1945.
12. Number of Holders of Cryptographic Materials December 1941 to October 1945.
13. The Converter M-134-C or SIGABA showing internal rotors. (The size is indicated by the standard typewriter keyboard.)
14. The Combined SIGCUM and SIGTOT installation. (The size is indicated by the standard typewriter keyboard.)
15. The Converter M-294 or SIGREM. (The size is indicated by the standard typewriter keyboard.)
16. The Converter M-209 ready for use.
17. One end of a SIGSALY terminal. (The size is indicated by the standard telephone equipment.)

INDEX TO

THE ACHIEVEMENTS OF THE SIGNAL SECURITY AGENCY

IN WORLD WAR II

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

APPENDIX

A typical SSA unit at work.

RESPONSIBILITY FOR CODE AND CIPHER WORK IN THE U. S. ARMY 1861-1945

BEFORE 1861 — CHAOS

1861-1865 CIVIL WAR
- SIGNAL CORPS — MOBILE STATIONS IN THE FIELD; SOLUTION ACTIVITIES INCIDENTAL
- MILITARY TELEGRAPH CORPS — FIXED TELEGRAPH LINES; SOLUTION ACTIVITIES INCIDENTAL

1865-1898
- SIGNAL CORPS — CODE COMPILATION, NO SOLUTION

1898 SPANISH-AMERICAN WAR
- SIGNAL CORPS — EXISTING CODES USED, NO COMPILATION, LITTLE OR NO SOLUTION

1898-1917
- SIGNAL CORPS — CODE COMPILATION
- THE ADJUTANT GENERAL — ONE CODE COMPILED (1902)
- ARMY SERVICE SCHOOLS — SOME TRAINING IN SOLUTION, TOWARD END OF PERIOD

1917-1919 WORLD WAR I
- (IN WASHINGTON) MILITARY INTELLIGENCE DIVISION, GENERAL STAFF — COMPILATION; SOLUTION; SECRET INK WORK; SHORTHAND; G-2 COMMUNICATIONS
- (IN FRANCE) SIGNAL CORPS — COMPILATION; INTERCEPTION; DIRECTION-FINDING
- (IN FRANCE) G-2 AEF — SOLUTION OF GERMAN COMMUNICATIONS

1919-1929
- (IN NEW YORK) MILITARY INTELLIGENCE DIVISION — (WITH STATE DEPT. SUPPORT); SOLUTION
- (IN WASHINGTON) SIGNAL CORPS — CODE COMPILATION
- (IN WASHINGTON) THE ADJUTANT GENERAL — PRINTING; DISTRIBUTION; ACCOUNTING

(ALL IN WASHINGTON HEREAFTER)

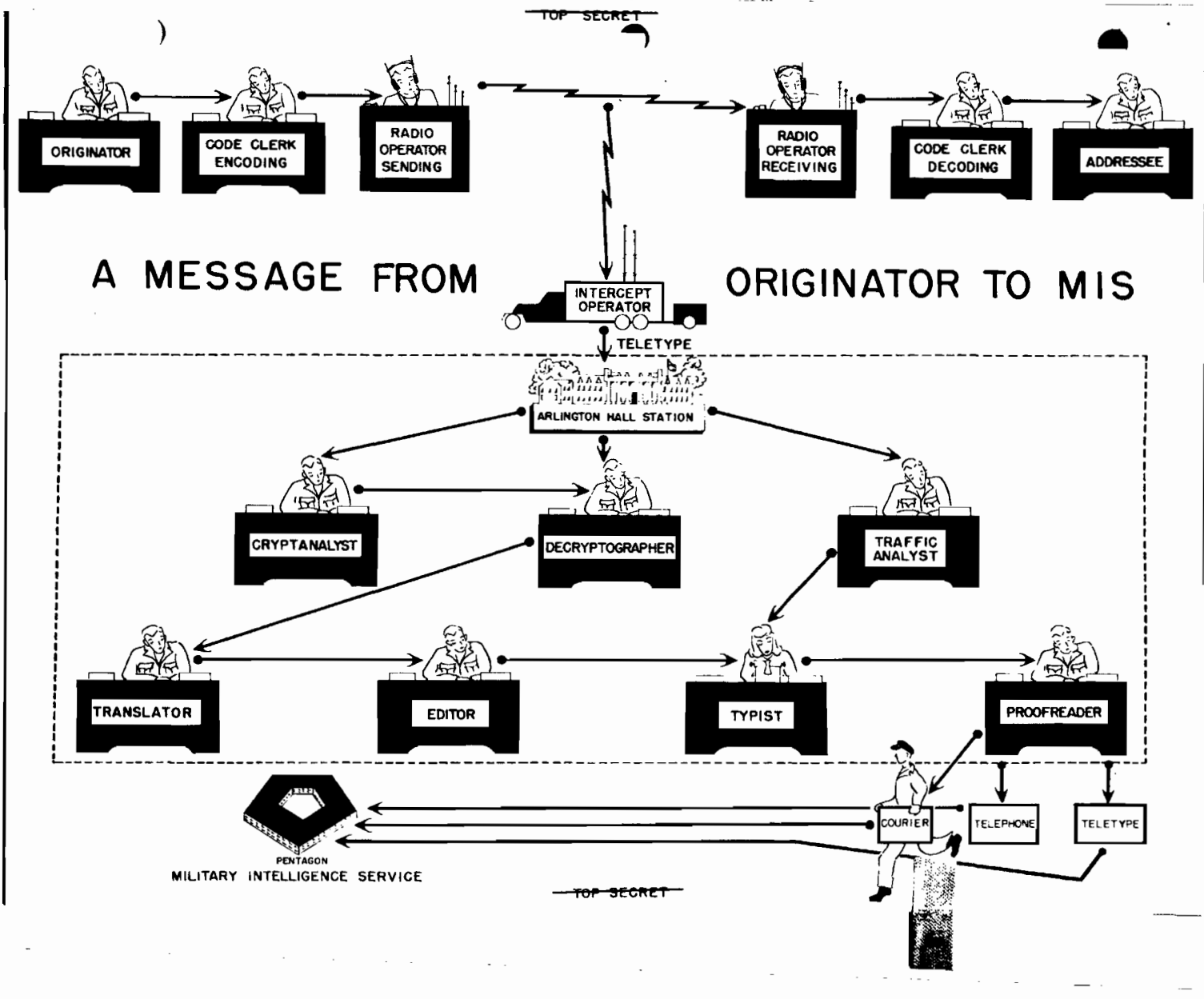
1930-1934
- SIGNAL CORPS, SIGNAL INTELLIGENCE SERVICE — CODE COMPILATION; TRAINING IN SOLUTION; GENERAL TRAINING; RESEARCH AND DEVELOPMENT
- THE ADJUTANT GENERAL — PRINTING; DISTRIBUTION; ACCOUNTING
- G-2 — STAFF SUPERVISION

1934-1941
- SIGNAL CORPS, SIGNAL INTELLIGENCE SERVICE — CODE COMPILATION; TRAINING IN SOLUTION; GENERAL TRAINING; INTERCEPTION; CURRENT SOLUTION; RESEARCH AND DEVELOPMENT; PRINTING; DISTRIBUTION; ACCOUNTING
- G-2 — STAFF SUPERVISION

1941-1944 WORLD WAR II
- SIGNAL CORPS — ALL PHASES OF ACTIVITY THROUGH SIGNAL SECURITY AGENCY AND SECOND SIGNAL SERVICE BATTALION AT ARLINGTON HALL STATION AND INTERCEPT STATIONS
- G-2 — STAFF SUPERVISION

DEC. 1944 - SEPT. 1945
- SIGNAL CORPS — ADMINISTRATIVE CONTROL OF ALL PHASES
- G-2 — OPERATIONAL CONTROL OF ALL PHASES

SEPT. 1945-
- G-2 — COMPLETE CONTROL OF ALL PHASES THROUGH ARMY SECURITY AGENCY AND SECOND SIGNAL SERVICE BATTALION AT ARLINGTON HALL STATION, INTERCEPT STATIONS AND THEATERS



Gen. Marshall's Letters to Gov. Dewey

By The Associated Press.

WASHINGTON, Dec. 7—Following are the texts of two letters General Marshall sent to Governor Dewey on Sept. 25, 1944, and Sept. 27, 1944, concerning the breaking of secret Japanese codes:

FIRST LETTER

TOP SECRET
(FOR MR. DEWEY'S EYES ONLY)

25 September, 1944.

My Dear Governor:

I am writing you without the knowledge of any other person except Admiral King (who concurs) because we are approaching a grave dilemma in the political reactions of Congress regarding Pearl Harbor.

What I have to tell you below is of such a highly secret nature that I feel compelled to ask you either to accept it on the basis of your not communicating its contents to any other person and returning this letter or not reading any further and returning the letter to the bearer.

I should have preferred to talk to you in person but I could not devise a method that would not be subject to press and radio reactions as to why the Chief of Staff of the Army would be seeking an interview with you at this particular moment. Therefore, I have turned to the method of this letter, to be delivered by hand to you by Col. Carter Clark who has charge of the most secret documents of the War and Navy Departments.

In brief, the military dilemma resulting from Congressional political battles of the political campaign is this:

The most vital evidence in the Pearl Harbor matter consists of our intercepts of the Japanese diplomatic communications. Over a period of years our cryptograph people analyzed the character of the machine the Japanese are using for encoding their diplomatic messages. Based on this, a corresponding machine was built by us which deciphers their messages.

Therefore, we possessed a wealth of information regarding their moves in the Pacific which in turn was furnished the State Department—rather than, as is popularly supposed, the State Department providing us with the information—but which unfortunately made no reference whatever to intentions toward Hawaii until the last message before Dec. 7, which did not reach our hands until the following day, Dec. 8.

Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.

To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the Battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate on our limited forces to meet their advances on Midway when otherwise we almost certainly would have been some 3,000 miles out of place.

We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.

Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys.

The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point.

The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

You will understand from the foregoing the utter tragic consequences if the present political debates regarding Pearl Harbor disclose to the enemy, German or Jap, any suspicion of the vital sources of information we now possess.

The Roberts' report on Pearl Harbor had to have withdrawn from it all reference to this highly secret matter, therefore in portions it necessarily appeared incomplete. The same reason which dictated that course is even more important today because our sources have been greatly elaborated.

As a further example of the delicacy of the situation, some of Donovan's people (the OSS), without telling us, instituted a secret search of the Japanese Embassy offices in Portugal. As a result the entire military attaché Japanese code all over the world was changed, and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable source of information, particularly regarding the European situation.

A recent speech in Congress by Representative Harness would clearly suggest to the Japanese that we have been reading their codes, though Mr. Harness and the American public would probably not draw any such conclusion.

The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the savings of American lives, both in the conduct of current operations and in looking toward the early termination of the war.

I am presenting this matter to you, for your secret information, in the hope that you will see your way clear to avoid the tragic results with which we are now threatened in the present political campaign. I might add that the recent action of Congress in requiring Army and Navy investigations for action before certain dates has compelled me to bring back the corps commander, General Gerow, whose troops are fighting at Trier, to testify here while the Germans are counter-attacking his forces there. This, however, is a very minor matter compared to the loss of our code information.

Please return this letter by bearer. I will hold it in my secret file subject to your reference should you so desire.

Faithfully yours,
G. C. MARSHALL.

Second Letter

TOP SECRET
(FOR MR. DEWEY'S EYES ONLY)

27 September, 1944.

My Dear Governor:

Colonel Clark, my messenger to you of yesterday, Sept. 26, has reported the result of his delivery of my letter dated Sept. 25. As I understand him you (A) were unwilling to commit yourself to any agreement regarding "not communicating its contents to any other person" in view of the fact that you felt you already knew certain of the things probably referred to in the letter, as suggested to you by seeing the word "cryptograph," and (B) you could not feel that such a letter as this to a Presidential candidate could have been addressed to you by an officer in my position without the knowledge of the President.

As to (A) above I am quite willing to have you read what comes hereafter with the understanding that you are bound not to communicate to any other person any portions on which you do not now have or later receive factual knowledge from some other source than myself. As to (B) above you have my word that neither the Secretary of War nor the President has any intimation whatsoever that such a letter has been addressed to you or that the preparation or sending of such a communication was being considered.

I assure you that the only persons who saw or know of the existence of either this letter or my letter to you dated Sept. 25 are Admiral King, seven key officers responsible for security of military communications, and my secretary who typed these letters.

I am trying my best to make plain to you that this letter is being addressed to you solely on my initiative, Admiral King having been consulted only after the letter was drafted, and I am persisting in the matter because the military hazards involved are so serious that I feel some action is necessary to protect the interests of our armed forces.

(The second letter then repeated the text of the first letter except for the first two paragraphs.)

THE NEW YORK TIMES
8 Dec. 1944
Page 5

SECRET

From: Berlin (GMBRK)
To: Tokyo (Summer)
9 November 1943
JAS

#878 Parts 14 - 17[a]

Summary of the organization of the strong points:

They utilize machine gun fire from several armored machine gun turrets and two or three armored machine gun casemates which, skillfully located in accordance with the terrain, can be used for flanking fire.

This fire is supplemented by the machine gun fire from the Ringstelle which are constructed everywhere.

(Part 15)

In order to eliminate dead space in the neighborhood of the strong points, they have two or three grenade throwers firing from within the armored turret ((?range?) 20 to 600 meters; speed of fire - 120 per minute; caliber, 50 mm. --G-- --G--. These are high-angle fire weapons.

For defense against tanks, tank ditches (built in triangular cross-section with a span across the top of 5 meters and a depth of 3.5 meters) are constructed along the periphery of the strong points.

SECRET

(Part 16)

In addition to having flanking fire provided by 2 or 3 casemates with 40 mm. Skoda anti-tank guns ((?similar to?) machine guns) and 2 or 3 casemates with 60 caliber 50 mm. anti-tank guns, they have 2 or 3 gun shelters (protected against bullets) with 60 caliber 50 mm. anti-tank guns which they can drag out into the open to fight when the opportune moment comes.

They also have mine fields in front of and behind the tank ditches (anti-tank mines, anti-personnel and horse mines, etc., are used together; they are laid in three rows of 2 mines each for each 3 square meters).

(Part 17)

As far as infantry obstacles are concerned, in addition to the mine fields, they have wire entanglements both in back of the tank ditches and within the strong points. For the direct protection of the casemates, fixed-type flame throwers are buried in the ground nearby and set up so that they can be electrically ignited from the Rinnstelle.

* - Part 10 not available; Parts 11 - 13 and 18 - 20 previously issued under same number; other Parts not yet readable.

SECRET

From: Berlin (Oshima)
To: Tokyo
10 August 1944
JAD

988 Urgent. (Three Parts Complete)

PART 1 Reference our #808.[a]

The following is the gist of a general statement on munitions production made to me by SPEER:

"1. At the time I assumed office as Munitions Minister as successor to TODT in 1942, I received various orders from HITLER regarding increased production of munitions, and at that time I received the impression that there was a spirit of listlessness generally in production circles. However, I discovered that the reason for that was that in each group of production leaders there were many from the management clique who could not rid themselves of the idea of profits, as it formerly existed. Therefore, I realized that it was necessary to replace them by persons who possessed a vigorous interest in the technical developments of production, and, making a clean sweep of these traditional leaders, I replaced them entirely by persons with technical interests. Also since there was no --1G-- the idea that there were also some superior persons among the technical officers in the army who might be used as

technicians, I employed them repeatedly[b] (with the object of (? gaining ?) versatility and elasticity).

"2. Then, in order to increase production, I emphasized particularly economy of raw materials and use of substitute materials. For example, I presented a program of increased production for tanks, airplanes, etc., in accordance with HITLER's orders at the time I took over. During this time, for example, they did such an irrational thing as to demand a greater quantity of copper than was produced in the whole world. However, as to actual accomplishments since then, there has been no important change in the amount of copper used, and it is clear from the accompanying table that aircraft and tanks have followed the road of increased production shown by the whole production picture. Moreover, since it was convenient to use ball bearings, it came to be almost a fad to do so and they were used even where it was not necessary, but I forbade this (? entirely ?), with the result that at present, although ball bearing production has been reduced to 42% of the maximum through the effect of air raids, there has been, needless to say, no effect at all on increased production of tanks, aircraft, and other things."

PART 2 3. Then SPEER explained the production situation in the various categories of his outline. In a word, taking production at the outbreak of the war as a norm, each category shows a gradually rising curve; toward the end of 1943 its rate generally slackens, but rising early this year, the curve becomes rather sharp. In June and July the rise becomes abrupt. However, because of the effect of air raids during that time there are several dips. (I shall wire a synthesis of the effect of air raids in a supplementary wire.) Coal and automobiles are cases where there is no particular change, with production remaining almost stagnant (however, even these have increased slightly); it seems the reason for the former is chiefly lack of man power, while the latter is largely the result of air raids. The fact that there is a marked decline in production of ball bearings, as mentioned above, and the various problems relating to oil are matters about which I shall wire later along with the problem of raw materials.

4. Among the miscellaneous remarks made by SPEER in his exposition of this outline, the following points are for your information:

(a) Monthly production of small arms ammunition at present: 600,000,000 rounds.

(b) Machine guns, new type: 20,000; old type: 5,000

(c) Light howitzers (10.5 centimeter): 1,000. (SPEER said that the goal set by HITLER when he ordered him to increase production was 300.)

(d) Heavy howitzers (15 centimeter): 300.

(e) Assault guns[c]. With the objective of giving them greater speed than tanks so that they may pursue and destroy them, every effort is being made to increase production of the 15-ton type rather than the old 25-ton type, and when it is possible to produce the latter in quantity--the monthly rate should reach 1,000 in February of next year--it is planned to discontinue the so-called PAK entirely and to make only this assault gun.

(f) There are three types of anti-aircraft guns: 8.8 centimeter, 10.5 centimeter, and 12.6 centimeter. The initial velocity of the latter is 1,300 meters; while it is useful for a great distance, its firing rate is --1G--. The 8.8 centimeter gun until recently had an initial velocity of 1000 meters and did not carry far. Its deviation was also great, but as a result of recent researches it has achieved an initial velocity of 1300 meters and its deviation

is not greatly different from that of the 12.6 centimeter gun. Therefore hereafter the main emphasis will be given to the 8.8 centimeter gun.

PART 3 (g) In general the German ordnance people have been in difficulty because the Germans had three types of gun: the 10.5 centimeter light howitzer, the 8.8 centimeter anti-aircraft gun, and the 7.5 centimeter anti-tank gun, whereas the fact that the Russians have unified them to 7.6 centimeters has been one of their strong points.

(h) There are two types of anti-aircraft machine gun: the 37 millimeter and the 20 millimeter. Since the latter does not have great effect, the former must be greatly increased. The fact that the initial velocity of those formerly used by the Germans was small was a defect, but since then they have gradually achieved success in research, even though it is not yet completely out of the experimental stage and there is no --U-- announcement of quantity production, and they are working hard to increase production of this weapon. Furthermore, ammunition is being improved and they have (? replaced ?) the shell which was ordinarily used in the past by a high explosive shell (? which causes a much greater explosion ?), with the result

that its effect is tremendously (? increased ?).

(i) In the past they used two types of searchlight, one of 1.5 meters and one of 2 meters. The latter was preferred because it could throw a (? small ray ?)[d] a great distance, and, since by further research it has been demonstrated that this one has almost --1G-- the efficiency of the former, it is planned to produce this one type.

5. [e]"While German munitions production in such things as aircraft will virtually reach its quantitative peak at the end of this year, I am making it a basic principle to hold to a rising curve, however slight, and because of the necessities of the future we cannot venture to provide for a fall in the curve in the future. That is to say, even though the war continues --1G-- years in --1G-- within Germany, it is planned that fighting power will not decline in so far as munitions production is concerned. However, if circumstances force it, (? we may have to curtail ?) complete tests of such things as the above-mentioned anti-aircraft machine gun and take them from the laboratory into quantity production."

a- SSA #134605.

b- Or "all".

c- STURM GESCHUTZ.

d- SHŌSHA.

e- This section seems to be a direct quotation of SPEER's remarks.

705

From: Hanoi
To: Tokyo
22 January 1945
JBB

J-16

B.A.

Re: your wire 67.[a] (Office Wire.)

I am rewiring, as follows: this company suggested commencing mining operations according to the plan below immediately after discovery of the Uranium vein. This will require a large amount of money for operations, and we are holding off operations until we get instructions from you, so please reply at once.

1. The Uranium vein which was discovered at this time (?can produce?) an estimated 50 kilograms of pure ore, and gives promise, as prospecting continues, of greatly increasing its output. Hence, we expect positive aid from the Industrial Council[b] for this mining.

2. This ore must be acquired at once, and so without waiting for the general result of our prospecting, we plan to carry out our project as in #1 following.

(1) November and December, preparation for mining operations to be made. (20,000 piasters (?are being used for?) building workmen's barracks, clearing away the ground for digging operations, etc.).

March and April, mining operations to be begun.

(2) For the time being the goal for mining pure Uranium ore is 15 to 50 kilogrammes. Yield of pure Uranium will be about 10%.

(3) One part of this needed material is expected to be taken over and supplied through the army here. (For each ton of explosive, 3 --1 line G--.)

(4) In short, total expenses will be 72,000

piasters.

(?5?) I shall soon be able to send you samples by plane. Please find out the quality of them.

Please make contacts for us in the matter of the telegraphic request which the SHIN Unit wired to Headquarters.

Also please wire instructions as to the future --1G-- expected quantity and maximum price of the ore.

a - Not available.
b - KOGYO KYOGIKAI.

WAR DEPARTMENT

TOP SECRET ULTRA

~~TOP SECRET ULTRA~~

4793, 4794, 4795

From: Moscow (SATO)
To : Tokyo
29 July 1945
JAA-2 - JAJ

1476 (3 part message complete)

Very Urgent.

PART 1: Re: your wire 944[a].

1. This wire (a repeat wire was received and read on the 28th) crossed with my wires 1449[b], 1450[c], and 1458[d]. On the same day the new Prime Minister, Mr. ATTLEE, returned to Potsdam and immediately participated in the Conference. Hence, there is nothing to be done about the proposal in 1 of your wire. Furthermore, if we should make such representations to Moscow, and if the Soviet officials find no reason to approve my trip, we will only be betraying our feelings of uneasiness.

2. In 2 of your wire, you say that I am to request the good offices of the Soviet Union, and that if the Soviet Union shows a cold attitude, it will make it inevitable to consider other ways and measures; and you feel that we might get a satisfactory arrangement by either flattering the Soviet Union or taking her down. However, in view of the general state of affairs, such an approach would seem to me to be lacking in soundness.

3. The American spokesmen[e] spoke firmly for an unconditional surrender, but he certainly hinted that if we were to accept this, in actual practice the terms would be toned down and indeed if we take this sort of meaning from it, we have the situation I expressed in my wire 1427[f].

Japanese Spec 011
Page 1

TOP SECRET ULTRA

~~TOP SECRET ULTRA~~
WAR DEPARTMENT

PART 2:

Although I don't know to what extent the radio broadcast of Naval Captain ZACHARIAS is authoritative, the principle enunciated by him that Japan will be able to reap the benefits of the Atlantic Charter differs from the attitude taken towards Germany before the capitulation of that nation. Germany was denied any right to partake in the Charter. While, in considering the reasons for the refusal towards Germany, no reasons appear for the present softening attitude towards Japan, there is the difference that we have no objection to the idea of restoration of world peace on the basis of the Charter. This raises a question as to whether the Imperial Government has already accepted disarmament, and whether, apart from the sending of the Special Envoy, somehow or other when a representation is made, notification shall be given at the outset that we will consent to disarmament. There is a similar question about prior recognition of the independence of Korea.

4. Your Excellency published a statement to the effect that the Japanese Government has decided to ignore the Three-Power ultimatum served on Japan on the 26th. BBC has broadcast statements on the matter, but as yet I have received no official wire. Furthermore, (? whether or not ?) we treat it with silent contempt, or publicize it in our ordinary reports, it is still a public expression of the intentions of England, America and China, and is the basis for the statements made by Captain ZACHARIAS.

PART 3:

In fact there are discrepancies in its important points. (In this declaration it is understood that while Japan's territory is to be limited to Honshū, Shikoku, Kyūshū and the Hokkaidō, America is to keep Okinawa in reserve as her own possession.)

TOP SECRET ULTRA

5. Your wire 893[g] deals merely with the sending of a Special Envoy, but in your 931[h], I am told to seek the good offices of the Russian Government. Again in your 944[i], I am to make clear that the sending of a Special Envoy is to get STALIN to consent to become a peace proposer, a fact, which I regret to say, indicates that we have been too stingy in giving them our plans. Furthermore, while the contingency that the Russians may manifest an indifferent attitude also is to be considered, (? unfortunately ?) I feel deeply perplexed because I am unable to think that other courses or means would suffice to accomplish anything.

6. To sum up, I am waiting for a reply from the Russians to the representation referred to in my 1450[c], and if none comes during the 30th (Monday), I will press them for one without delay.

7. I had no sooner finished drafting this message than I received your 952[j]. As for the interview with MOLOTOV referred to in (3), if our Imperial Government has a concrete and definite plan for bringing the war to an end, I would like to be informed in a special way; otherwise I will go ahead on the basis of (1) of this message.

a - H-198547.
b - Spec 002 and H-198553.
c - Spec 001.
d - Spec 009.
e - In English.
f - H-197715.
g - H-196285.
h - H-197837.
i - H-198547.
j - Spec 007.

Inter 2212Z 29 Jul 45 (?) Japanese Spec 011
Rec'd 30 Jul 45 Page 3
Trans 1255 30 Jul 45 (1031-1227-t)
JNU3 de RTZ,

TOP SECRET ULTRA

DOCID: 3400833

SECRET

TL KG-56...

From: ?
To: ?
11 August 1943
JCM

#0198 Part III

Message #0198 Part III

Paragraph 2:

Leaving Palau August 16th

Unloading at Hewak September 1st 2...

--U-- Transport #3795 (0416)

#8361 (0694)

#9591 (0426)

#2781

Army transport ship --U-- --U-- 1 ship --U--

Total - 6 ships

End part

a - Type of Ship

b - RIKIGUN UNYU SH...

...Aug 43 (14) Japanese JR #4335
Rec'd 12 Aug 43
Trans 20 Aug 43 (J70-hr)

SECRET

This sheet and all of the information contained in this message must be safeguarded with the greatest care. Unauthorized persons must be prevented from drying up this sort of vital intelligence at its source.

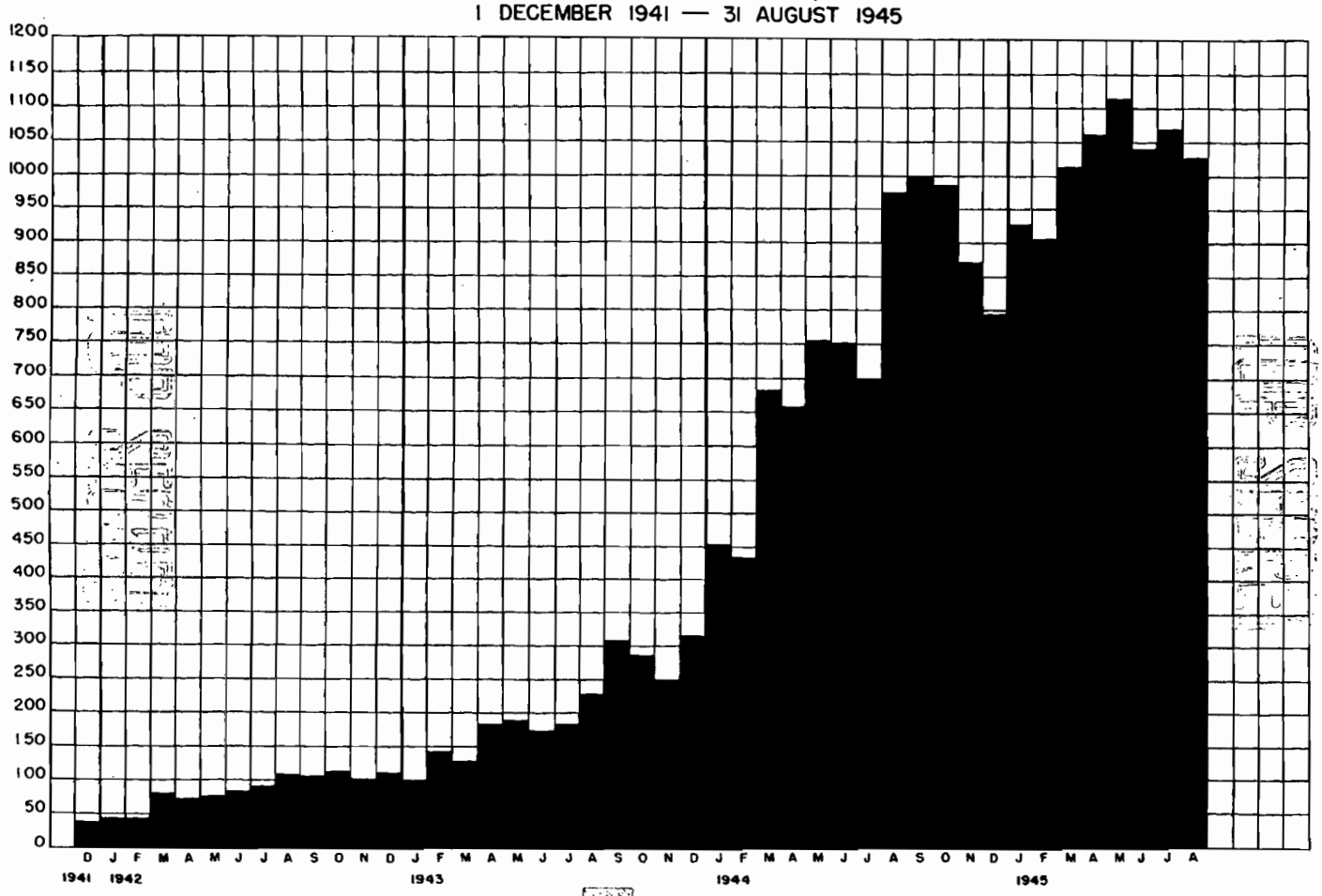
DOCID: 3480833

TOP SECRET

BULLETIN PRODUCTION

AVERAGE DAILY VOLUME OF TRANSLATED MESSAGES

1 DECEMBER 1941 — 31 AUGUST 1945



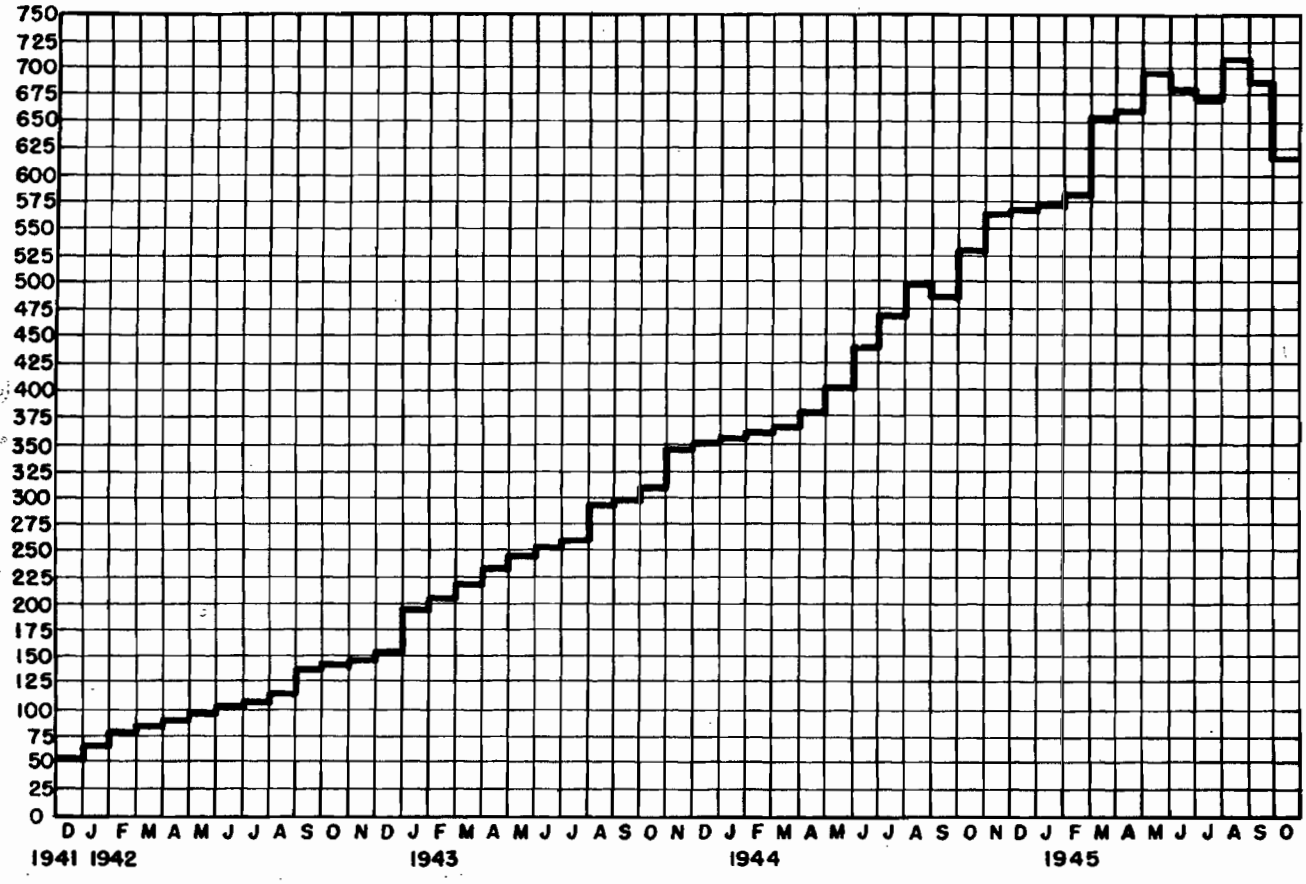
TOP SECRET

DOCID: 3480833

~~TOP SECRET~~

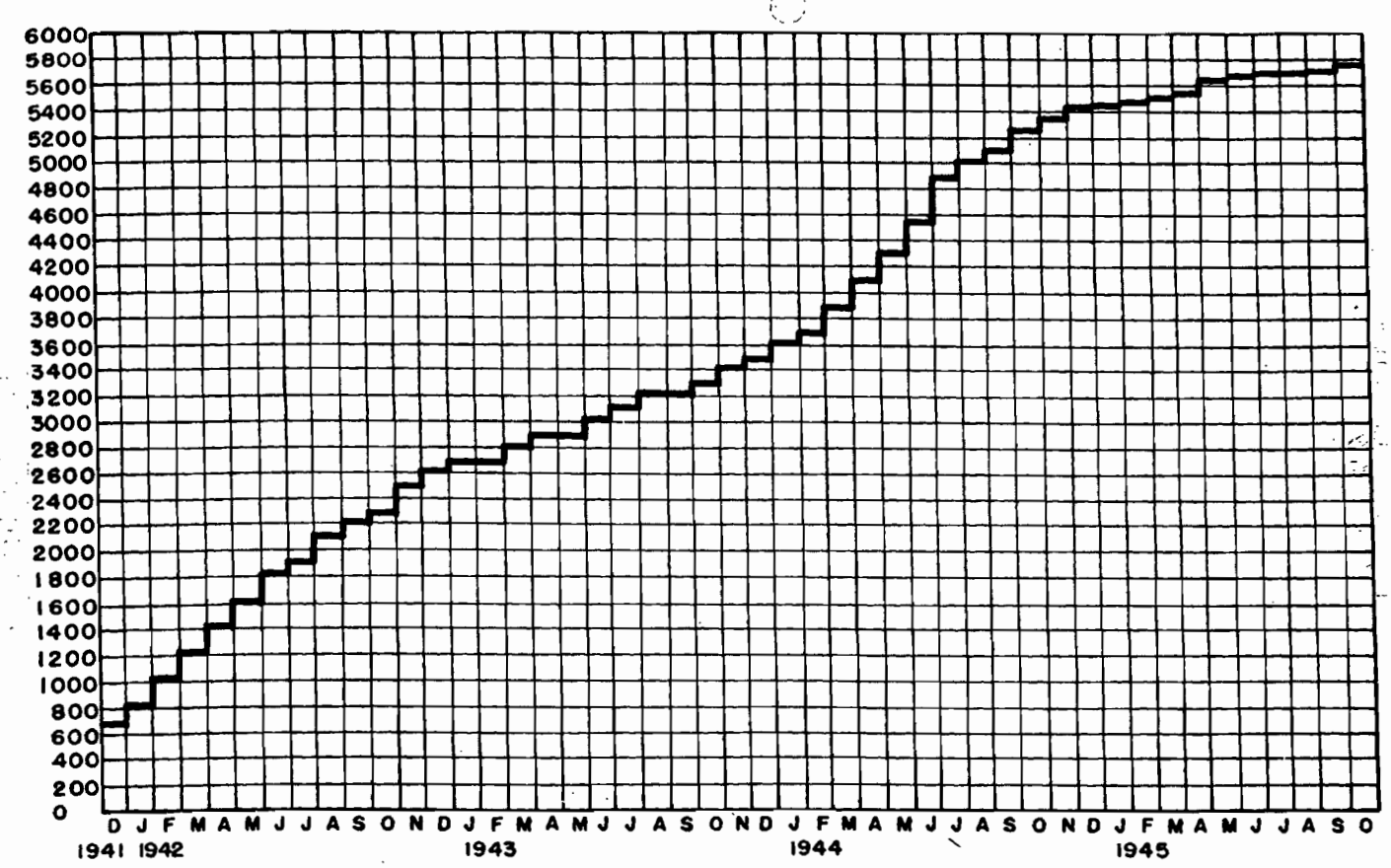
NUMBER OF CRYPTOGRAPH) SYSTEMS IN EFFECT

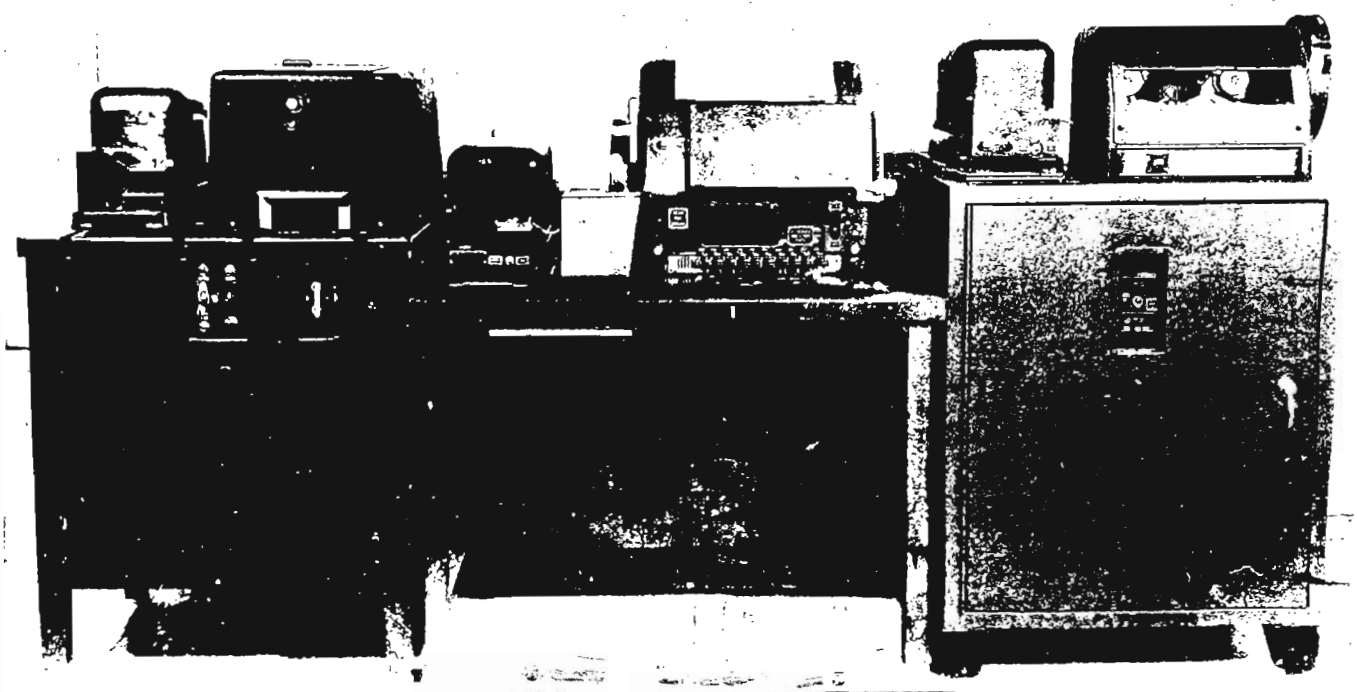
7 DECEMBER 1941 — OCTOBER 1945



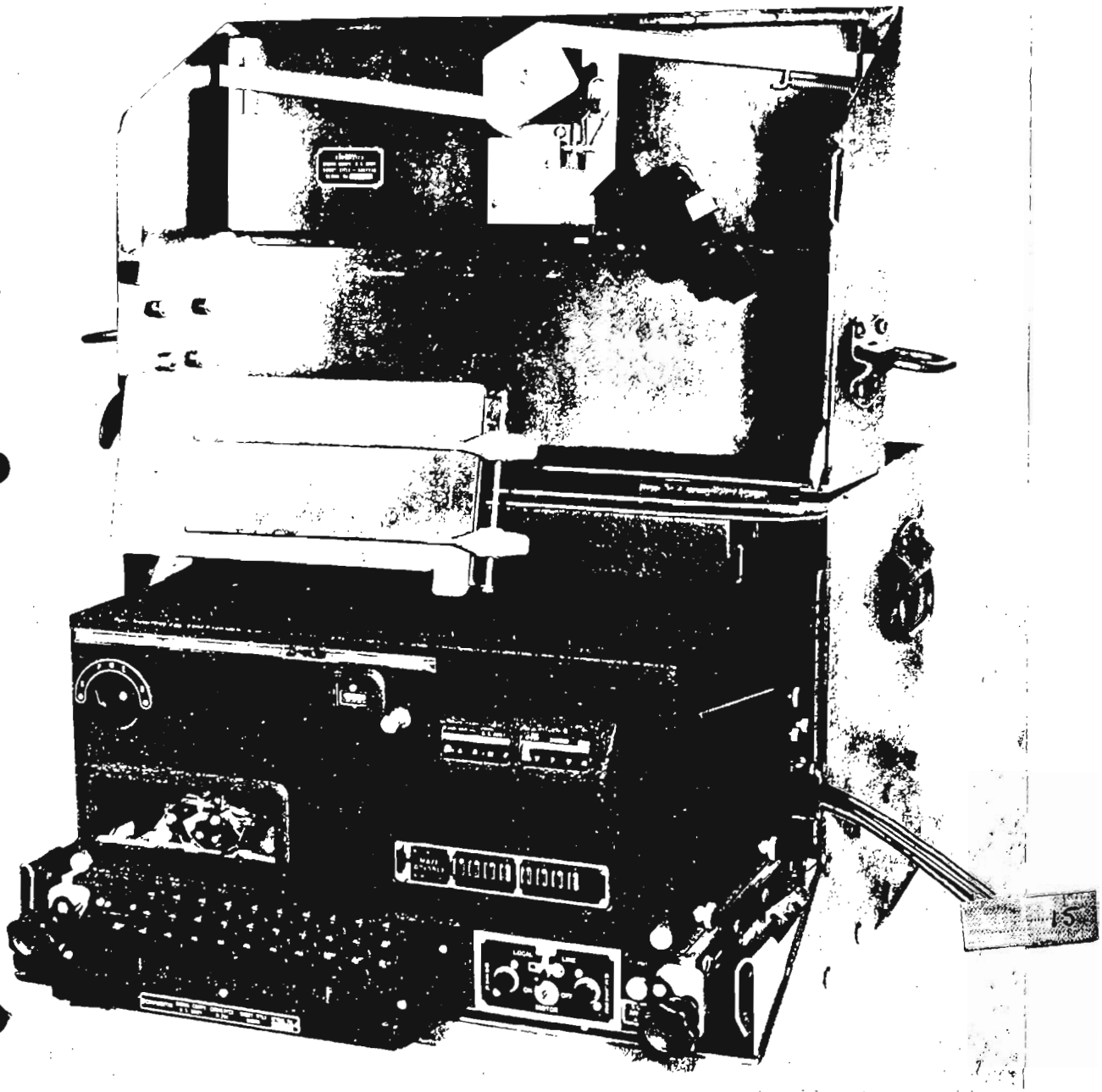
~~TOP SECRET~~

NUMBER OF HOLDERS OF CRYPTOGRAPHIC MATERIALS
DECEMBER 1941 — OCTOBER 1945



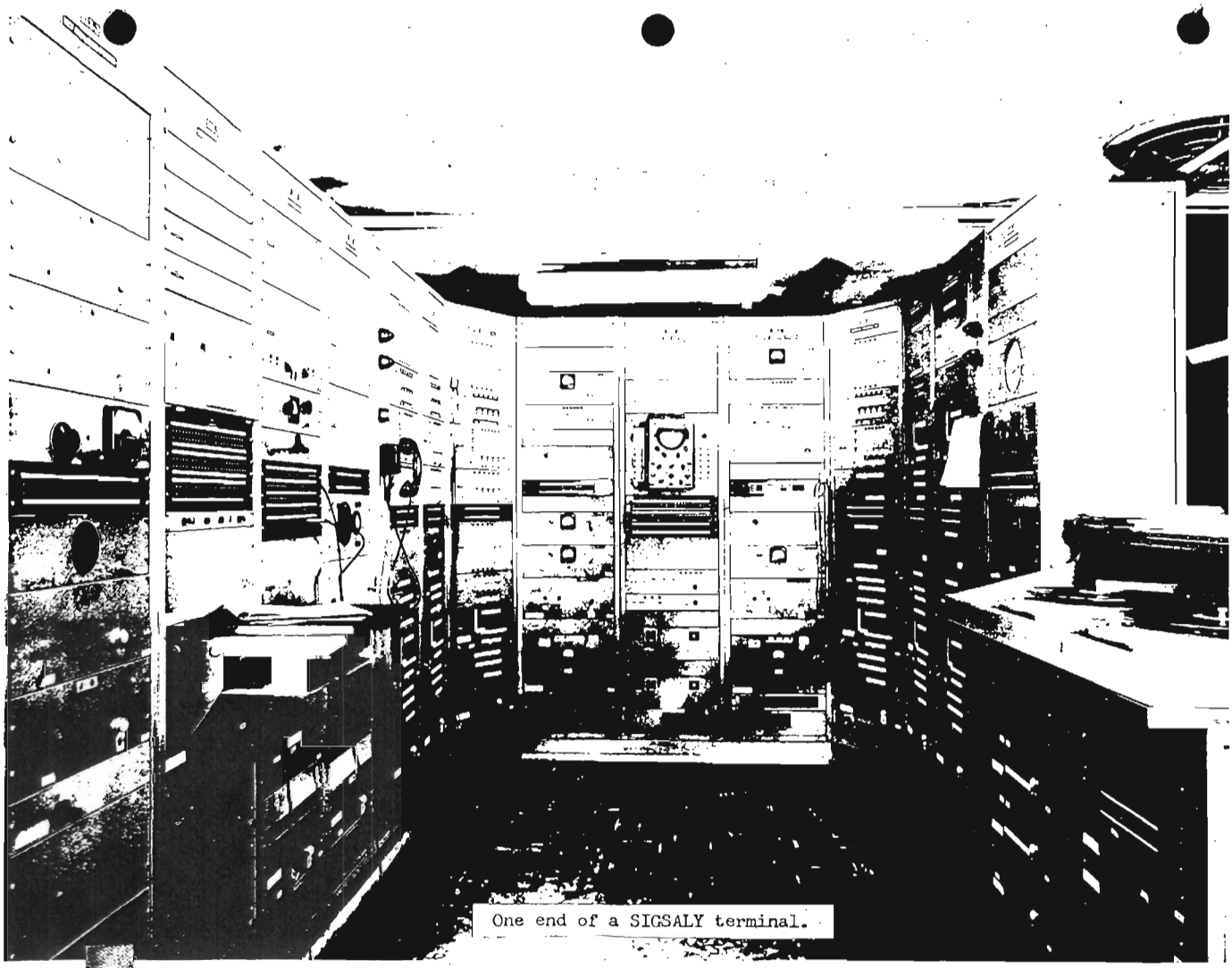


The Combined SIGCUM and SIGTOT installations.



The Converter M-294 or SIGNIN.

The Converter M-209 ready for use.



One end of a SIGSALY terminal.